A MITEL
PRODUCT
GUIDE

Mitel OpenScape Business

OpenScape Business V3

Administrator Documentation
03/2026

A31003-P3030-M100-65-76A9

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 2026, Mitel Networks Corporation

All rights reserved

Contents

1 History of changes **38**
1.1 History of improvements/fixes 56

2 Introduction and Important Notes **65**
2.1 About this Documentation 65
2.1.1 Documentation and Target Groups 65
2.1.2 Structure of the Administrator Documentation 67
2.1.3 Types of Topics 69
2.1.4 Display Conventions 69
2.2 Safety Information and Warnings 70
2.2.1 Warnings: Danger 71
2.2.2 Warnings: Warning 71
2.2.3 Warnings: Caution 72
2.2.4 Warnings: Note 73
2.2.5 Country-specific Safety Information 74
2.2.5.1 Safety Information for Australia 74
2.2.5.2 Safety Information for Brazil 74
2.2.5.3 Safety Information for the U.S 75
2.2.5.4 Safety Information for Canada 77
2.3 Important Notes 77
2.3.1 Emergencies 78
2.3.2 Proper Use 78
2.3.3 Correct Disposal and Recycling 79
2.3.4 Installation Standards and Guidelines 80
2.3.4.1 Connecting OpenScape Office X to the Power Supply Circuit 80
2.3.4.2 Connecting OpenScape Business S and OpenScape Business UC Booster Server to the Power Supply Circuit 80
2.3.4.3 Shielded Cabling for LAN and WAN Connections of OpenScape Business X 80
2.3.4.4 Fire Safety Requirements 81
2.3.4.5 Lightning Protection Requirements 81
2.3.4.6 Markings for OpenScape Business X 82
2.3.5 Notes on Electromagnetic and Radio Frequency Interference of OpenScape Business X 82
2.3.6 Data Protection and Data Security 82
2.3.7 Technical Regulations and Conformity of OpenScape Business X 83
2.3.7.1 CE Conformity 84
2.3.7.2 Conformity with US and Canadian Standards 84
2.3.7.3 Conformity with International Standards 84
2.3.8 Operating Conditions 84
2.3.8.1 Operating Conditions for OpenScape Business X 85
2.3.8.2 Operating Conditions for OpenScape Business S and OpenScape Business UC Booster Server 85

3 System Overview **86**
3.1 Highlights 86
3.2 Unified Communications 86
3.2.1 UC Features (Overview) 87
3.2.2 User Access to UC Features (UC Clients) 93
3.2.3 Integration in Business Applications 96
3.3 OpenScape Business Models 97
3.3.1 Expansion Levels Available through Sales 97
3.3.2 UC Hardware Models 101

3.3.3 UC Booster Hardware....102
3.3.4 UC Software Models (Softswitch)....102
3.3.5 Structure and Environmental Conditions....102
3.3.6 Supported Phones....103
3.4 Further information....104
3.4.1 Languages Supported....104
3.4.2 Internet Links....106

4 Administration Concept....108
4.1 OpenScape Business Assistant (WBM)....108
4.1.1 Requirements for the WBM....108
4.1.2 Home Page of the WBM....108
4.1.3 Introduction to the WBM....110
4.1.3.1 How to Log into the WBM....112
4.1.3.2 How to Log out from the WBM....112
4.1.4 WBM User Management....112
4.1.4.1 How to Add an Administrator....115
4.1.4.2 How to Edit an Administrator....116
4.1.4.3 How to Change your Own Administrator Password....116
4.1.4.4 How to Delete an Administrator....116
4.1.4.5 How to change a Manager E Administrator password....117
4.1.5 Wizards....117
4.1.5.1 Wizards – Basic Installation....117
4.1.5.2 Wizards – Network / Internet....118
4.1.5.3 Wizards – Telephones / Subscribers....118
4.1.5.4 Wizards – Central Telephony....119
4.1.5.5 Wizards – User Telephony....119
4.1.5.6 Wizards – Security....120
4.1.5.7 Wizards - UC Smart (only with UC Smart)....120
4.1.5.8 Wizards - UC Suite (only with UC Suite)....120
4.1.5.9 Wizards – Unified Directory....121
4.1.5.10 Wizards - Cloud Services....121
4.1.6 Service Center....122
4.1.6.1 Service Center – **Documents**....122
4.1.6.2 Service Center – **Software**....122
4.1.6.3 Service Center – **Inventory** > **System**....123
4.1.6.4 Service Center – **Inventory** > **Call Numbers**....123
4.1.6.5 Service Center – **Inventory** > **Network Overview**....123
4.1.6.6 Service Center – **Software Update**....123
4.1.6.7 Service Center – **E-mail Forwarding**....123
4.1.6.8 Service Center – **Remote Access**....123
4.1.6.9 Service Center – **Restart / Reload**....123
4.1.6.10 Service Center – **Diagnostics** > **Status**....124
4.1.6.11 Service Center – **Diagnostics** > **Event Viewer**....124
4.1.6.12 Service Center – **Diagnostics** > **Trace**....124
4.1.6.13 Service Center – Diagnostics > Service log....124
4.1.7 Expert Mode....124
4.1.8 Online Help....124
4.1.8.1 How to Invoke the Context-Sensitive Online Help....125
4.2 Manager E....125
4.2.1 How to Load the CDB into Manager E....126
4.2.2 How to Load the CDB Back into the System....126

5 Initial Setup for OpenScape Business X....128
5.1 Prerequisites for the Initial installation....128
5.2 Components....130

5.3 Dial Plan..... 131
5.4 IP Address Scheme..... 132
5.5 Initial Startup..... 134
5.5.1 How to Restart the Communication System..... 134
5.5.2 How to Connect the Admin PC to the Communication System..... 135
5.5.3 How to Start the WBM..... 136
5.6 Integration into the Customer LAN..... 137
5.6.1 How to Start the Initial Installation Wizard..... 137
5.6.2 System Settings..... 138
5.6.2.1 How to Set the Display Logo and the Product Name..... 138
5.6.2.2 How to Specify the IP Addresses (Optional)..... 139
5.6.2.3 How to Specify the Device Name..... 140
5.6.3 DHCP Settings..... 140
5.6.3.1 How to Disable the Internal DHCP Server..... 141
5.6.3.2 How to Enable and Configure the Internal DHCP Server..... 142
5.6.3.3 How to Enable DHCP for Mitel/Unify Devices Only..... 143
5.6.4 Country and Time Settings..... 144
5.6.4.1 How to Select the Country Code and the Language for Event Logs..... 145
5.6.4.2 How to Enter the DECT System ID..... 146
5.6.4.3 How to Set the Date and Time Manually..... 146
5.6.4.4 How to Obtain the Date and Time from an SNTP Server..... 147
5.6.5 UC Solution..... 148
5.6.5.1 How to Define the UC Solution..... 148
5.6.6 Connecting the Communication System to the Customer LAN..... 149
5.6.6.1 How to Connect the Communication System to the Customer LAN..... 149
5.7 Basic Configuration..... 150
5.7.1 How to Start the Basic Installation Wizard..... 150
5.7.2 System Phone Numbers and Networking..... 150
5.7.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection..... 151
5.7.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection..... 152
5.7.2.3 How to Activate or Deactivate Networking..... 152
5.7.3 Station Data..... 153
5.7.3.1 How to Display the Station Data..... 154
5.7.3.2 How to Delete all Call Numbers..... 155
5.7.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan..... 155
5.7.3.4 How to Import the Station Data from an XML File..... 156
5.7.3.5 How to display Mass data..... 156
5.7.4 ISDN Configuration..... 158
5.7.4.1 How to Configure the Connection of ISDN Stations..... 158
5.7.4.2 How to Configure the ISDN Point-to-Point Connection..... 159
5.7.4.3 How to Configure the ISDN Point-to-Multipoint Connection..... 159
5.7.4.4 How to Deactivate the ISDN Configuration..... 160
5.7.5 Internet Access..... 160
5.7.5.1 How to Configure Internet Access via an External Internet Router over the LAN Port..... 163
5.7.5.2 How to Configure Internet Access via an External Internet Router over the WAN Port..... 164
5.7.5.3 How to Configure Internet Access via a Preconfigured ISP..... 165
5.7.5.4 How to Configure Internet Access via the Standard ISP PPPoE..... 167
5.7.5.5 How to Configure Internet Access via a Standard ISP PPTP..... 169
5.7.5.6 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP..... 171
5.7.5.7 How to Disable Internet Access..... 172
5.7.6 Internet Telephony..... 173
5.7.6.1 How to Configure a Predefined ITSP..... 174
5.7.6.2 How to Deactivate Internet Telephony..... 178
5.7.7 Stations..... 179
5.7.7.1 How to Configure ISDN Stations..... 179

5.7.7.2 How to Configure Analog Stations ... 182
5.7.7.3 How to Configure UP0 Stations ... 184
5.7.7.4 How to Configure DECT Stations ... 187
5.7.7.5 How to Configure IP and SIP Stations ... 190
5.7.8 Configuring UC Suite ... 192
5.7.8.1 How to Configure the UC Suite ... 193
5.7.9 Configuring UC Smart Mailboxes ... 193
5.7.9.1 How to Configure UC Smart Voicemail Boxes ... 194
5.7.10 Conference Server Settings ... 194
5.7.10.1 How to Edit the Conference Server Settings ... 194
5.7.11 E-mail Delivery (Optional) ... 195
5.7.11.1 How to Configure the Sending of E-mails ... 195
5.8 Closing Activities ... 198
5.8.1 How to Activate and Assign the Licenses ... 198
5.8.2 How to Provision the UC Smart Client for Installation ... 201
5.8.3 How to Provision the UC Suite Clients for Installation ... 201
5.8.4 How to Perform a Data Backup ... 202
5.9 Commissioning of IP Phones ... 203
5.9.1 How to Configure an IP Phone ... 204
5.9.2 How to Configure a SIP Phone ... 206
5.10 How to collect diagnostic traces for error incident ... 207
5.11 Reflashing ... 208

6 Initial Setup for OpenScape Business S ... 211
6.1 Prerequisites for the Initial Setup ... 211
6.2 Components ... 213
6.3 IP Address Scheme ... 214
6.4 Dial Plan ... 215
6.5 Installing the Communication Software ... 216
6.5.1 How to Install the Communication Software ... 217
6.6 Starting Up ... 219
6.6.1 How to Start the Initial Installation Wizard ... 219
6.6.2 System Settings ... 220
6.6.2.1 How to Set the Display Logo and Product Name ... 220
6.6.2.2 How to Select the Country Code and the Language for Trace Logs ... 221
6.6.2.3 How to Activate an Additional LAN Port as a WAN Interface ... 222
6.6.2.4 How to Change the Dial Plan to 4 Digits ... 223
6.6.3 UC Solution ... 224
6.6.3.1 How to Define the UC Solution ... 224
6.7 Basic Configuration ... 225
6.7.1 How to Start the Basic Installation Wizard ... 225
6.7.2 System Phone Numbers and Networking ... 226
6.7.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection ... 226
6.7.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection ... 227
6.7.2.3 How to Activate or Deactivate Networking ... 228
6.7.2.4 How to Configure the Upstream of your Internet connection ... 228
6.7.3 Station Data ... 228
6.7.3.1 How to Display the Station Data ... 230
6.7.3.2 How to Delete all Call Numbers ... 230
6.7.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan ... 231
6.7.3.4 How to Import the Station Data from an XML File ... 232
6.7.4 Internet Access ... 232
6.7.4.1 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP ... 232
6.7.5 Internet Telephony ... 234
6.7.5.1 How to Configure a Predefined ITSP ... 235

6.7.5.2 How to Deactivate Internet Telephony....239
6.7.6 Stations....240
6.7.6.1 How to Configure IP and SIP Stations....240
6.7.7 Configuring UC Suite....242
6.7.7.1 How to Configure the UC Suite....243
6.7.8 Configuring UC Smart Mailboxes....243
6.7.8.1 How to Configure UC Smart Voicemail Boxes....244
6.7.9 Conference Server Settings....244
6.7.9.1 How to Edit the Conference Server Settings....244
6.7.10 E-mail Delivery (Optional)....245
6.7.10.1 How to Configure the Sending of E-mails....245
6.8 Closing Activities....248
6.8.1 How to Activate and Assign the Licenses....248
6.8.2 How to Provision the UC Smart Client for Installation....251
6.8.3 How to Provision the UC Suite Clients for Installation....251
6.8.4 How to Perform a Data Backup....252
6.9 Commissioning of IP Phones....253
6.9.1 How to Configure an IP Phone....254
6.9.2 How to Configure a SIP Phone....255
6.10 Uninstalling the Communication Software....256
6.10.1 How to Uninstall the Communication Software....257
6.11 Used Ports....257
6.12 How to collect diagnostic traces for error incident....259
6.13 Reflashing....260

7 Initial Setup of OpenScape Business UC Booster....263
7.1 Prerequisites for the Initial Setup....265
7.2 Backing up the Configuration Data of the Communication System....268
7.2.1 How to Perform a Data Backup....268
7.3 Commissioning the UC Booster Card....269
7.3.1 Installing the UC Booster Card....269
7.3.2 Configuring the UC Booster Card....269
7.3.3 Updating the Software for the UC Booster Card....270
7.3.3.1 How to Perform a Software Update....270
7.4 Commissioning the UC Booster Server....270
7.4.1 Installing the Communication Software....271
7.4.1.1 How to Install the Communication Software....272
7.4.2 Configuring the UC Booster Server....273
7.4.2.1 Announcing the IP Address of the Communication System....274
7.4.3 Updating the Software for the UC Booster Server....276
7.5 Basic Configuration....276
7.6 Closing Activities....276
7.7 Uninstalling the Communication Software....277
7.7.1 How to Uninstall the Communication Software....277
7.8 Upgrading from the UC Booster Card to the UC Booster Server....277
7.9 Used Ports....279

8 Licensing....282
8.1 Licensing Procedure....283
8.2 Licenses....285
8.2.1 Basic License....286
8.2.2 User Licenses....287
8.2.3 User-oriented Licenses....288
8.2.4 System Licenses....290
8.2.5 Evaluation Licenses....292
8.2.6 Upgrade Licenses....294

8.2.7 Possible License Combinations....294
8.3 Licensing a Communication System (Standalone)....297
8.3.1 CLS Connect....297
8.3.1.1 How to Activate CLS Connect....298
8.3.1.2 Switching from CLS connect....298
8.3.2 Activating Licenses (Standalone)....299
8.3.2.1 How to Activate Licenses Online (Standalone)....300
8.3.2.2 How to Activate Licenses Offline (Standalone)....301
8.3.3 Assigning Licenses (Standalone)....301
8.3.3.1 How to License Subscribers (Standalone)....303
8.3.3.2 How to License Trunks (Standalone)....306
8.4 Licensing Multiple Communication Systems (Internetwork)....306
8.4.1 License Activation (Internetwork)....308
8.4.1.1 How to Activate Licenses Offline (Internetwork)....309
8.4.1.2 How to Combine License Files into a Network License File....310
8.4.2 Assigning Licenses (Internetwork)....311
8.4.2.1 How to License Subscribers (Internetwork)....313
8.4.2.2 How to License Trunks (Internetwork)....316
8.4.2.3 How to Assign System Licenses to a Node....316
8.4.2.4 How to Assign the "Networking" System License to a Node....317
8.5 License information....317
8.5.1 License Information without a Network (Standalone)....317
8.5.1.1 How to Display License Information....318
8.5.2 License Information in an Internetwork....318
8.5.2.1 How to Display all Licenses in the Internetwork....318
8.5.2.2 How to Display the Licenses Bound to a Node....319
8.5.2.3 How to Display all Shared Licenses in an Internetwork....319
8.5.2.4 How to Display a Node-Dependent View of Station Licenses and User-Oriented Licenses....320
8.6 Assigning License Profiles....320
8.6.1 How to Add a License Profile....321
8.6.2 How to Edit a License Profile....321
8.6.3 How to Assign a License Profile to Stations....322
8.6.4 How to Delete a License Profile....323
8.7 Rehosting after Replacement of Hardware....323
8.7.1 How to Perform a Rehost after Replacing Hardware....324
8.8 License Server (Central License Server, CLS)....325
8.8.1 How to Check or Change the IP Address of the License Server....325
8.8.2 How to check Central License Server (CLS) Connection....325
8.9 Customer License Agent (CLA)....325
8.9.1 How to Configure the Connection to the Local License Agent....326
8.9.2 How to Change the Connection to the Central License Agent....326
8.10 Locking ID and Advanced ID Locking....326
8.10.1 How to Check the Locking ID of the Communication System....328
8.10.2 How to Check the Locking ID of the Softswitch....328
8.10.3 How to Check the Advanced Locking ID of Softswitches....328
8.11 How to migrate from V2 mainboard to V3 mainboard (standalone system)....328
8.12 How to migrate from V2 mainboard to V3 mainboard the master node of a networked system....330
8.13 How to migrate from V2 mainboard to V3 mainboard the slave node of a networked system....331
8.14 Migration of HiPath 3000 systems to OSBiz V3 software with V3 mainboard....331
8.15 Upgrade from V2 to V3 with **CLS Connect**....332
8.16 Upgrade from V2 to V3 without **CLS Connect**....332

9 Integration into the Internal Data Network (LAN)....333
9.1 LAN Interface....333
9.1.1 IP Address and Subnet Mask of the LAN Interface....333
9.1.1.1 How to Change the IP Address and Subnet Mask of the Hardware Platform....334

9.1.1.2 How to Change the IP Address of the UC Booster Card....334
9.1.1.3 How to Check or Change the IP Address and Subnet Mask of the Softswitch....335
9.1.2 Internal IP Address Range of the LAN Interface....335
9.1.2.1 How to Change the Internal IP Address Range of the Hardware Platform....336
9.1.2.2 How to Reset the Internal IP Address Range of the Hardware Platform....336
9.2 DHCP....337
9.2.1 DHCP Relay Agent....337
9.2.1.1 How to Configure the Hardware Platform as a DHCP Relay Agent....337
9.2.2 DHCP Server....338
9.2.2.1 How to Enable and Configure the DHCP Server of the Hardware Platform....339
9.2.2.2 How to Disable the DHCP Server of the Hardware Platform....341
9.2.2.3 How to Enable and Configure the DHCP Server of the Softswitch....341
9.2.2.4 How to Disable the DHCP Server of the Softswitch....342
9.2.2.5 How to Enable DHCP for Mitel/Unify Devices Only....342
9.3 DNS - Name Resolution....344
9.3.1 How to Define an External DNS Server....346
9.4 IP Routing....346
9.4.1 How to Activate or Deactivate the Default Router....347
9.4.2 How to Add a Static Route....347
9.4.3 How to Delete Static Routes....348
9.5 Deployment Service (DLS and DLI)....348
9.5.1 How to Configure the External DLS Server in the Internal DHCP Server....350
9.5.2 How to Enable the Internal DLI....351
9.5.3 How to Configure the Communication System as a Deployment and Licensing Client....352

10 Connection to Service Provider....353
10.1 Internet Access....353
10.1.1 Internet Access via an External Internet Router....355
10.1.1.1 How to Configure Internet Access via an External Internet Router over the LAN Port....356
10.1.1.2 How to Configure Internet Access via an External Internet Router over the WAN Port....356
10.1.1.3 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP....358
10.1.2 Internet Access via an Internet Modem....359
10.1.2.1 How to Configure Internet Access via a Preconfigured ISP....360
10.1.2.2 How to Configure Internet Access via a Standard ISP PPPoE....362
10.1.2.3 How to Configure Internet Access via a Standard ISP PPTP....364
10.1.3 WAN port....367
10.1.4 DynDNS....367
10.1.4.1 How to Configure the DynDNS Service....368
10.1.4.2 How to Define the Mail Exchanger....369
10.2 CO Access via ITSP....370
10.2.1 Configuring an ITSP....371
10.2.1.1 How to Configure a Predefined ITSP....373
10.2.1.2 How to Add a New ITSP....379
10.2.1.3 How to Configure Multi-Sites over ITSPs....385
10.2.1.4 How to Save a Preconfigured ITSP Template as a New Template....386
10.2.1.5 How to Customize a Preconfigured ITSP Template....386
10.2.1.6 How to Manually Update a Preconfigured ITSP Template....387
10.2.2 STUN (Simple Traversal of UDP through NAT)....388
10.2.2.1 How to Set the STUN Mode....388
10.3 CO Access over Digital and Analog Lines....389
10.3.1 Trunks....389
10.3.1.1 How to Configure an ISDN Outside Line....390
10.3.1.2 How to Configure an Analog Outside Line....391
10.3.1.3 How to Display All Trunks....392
10.3.1.4 How to Display Individual Trunks....392

10.3.1.5 How to Change the Trunk Code....393
10.3.1.6 How to Assign an MSN to a Trunk....393
10.3.1.7 ISDN protocol, modify....393
10.3.1.8 How to Change the B Channel Seizure Mode....394
10.3.1.9 How to Change the Dialing Method....394
10.3.2 Routes....394
10.3.2.1 How to Change a Route Assignment....397
10.3.2.2 How to Change the Route Name....398
10.3.2.3 How to Change the Seizure Code....398
10.3.2.4 How to Configure an Overflow Route with LCR Disabled....398
10.3.2.5 How to Configure an Overflow Route with LCR Enabled....399
10.3.2.6 How to Configure the Type of Seizure....399
10.3.2.7 How to Enter the PABX Number Incoming and Outgoing....399
10.3.2.8 How to Configure the Format of the Transmitted Call Number....400
10.3.2.9 How to Configure the Type of the Transmitted Call Number....400
10.3.2.10 How to Configure the Direction Prefix....400
10.3.2.11 How to Define a Route for Networking and Enter a Second CO Code....401
10.3.3 Dial Tone Monitoring....401
10.3.3.1 How to Configure a Delay Period for Dial Tone Monitoring....402
10.3.3.2 How to Configure the Dial Tone Monitoring Time....403
10.3.3.3 How to Configure the Digit Dial Time....403
10.3.3.4 How to Enable or Disable the Analysis of the Second Dial Tone....404
10.4 Prioritizing the Exchange Line Seizure with LCR Enabled....404
10.4.1 How to Prioritize the Seizure of Exchange Lines....404

11 Stations....406
11.1 Dial Plan....406
11.1.1 Default Dial Plan....407
11.1.2 Individual Dial Plan....408
11.1.2.1 How to Delete or Edit Default Phone Numbers....408
11.1.2.2 How to Edit Special Default Call Numbers....409
11.1.2.3 How to Import Call Numbers and Station Data....410
11.2 LAN Telephony Requirements....411
11.2.1 Audio Codecs....411
11.2.1.1 How to Configure Audio Codec Parameters....412
11.2.1.2 How to Assign Audio Codec Parameters to a Destination....413
11.2.2 Transmission of Tones According to RFC 2833....414
11.2.2.1 How to Enable or Disable Transmission of Fax/Modem Tones According to RFC2833....414
11.2.2.2 How to Enable or Disable Transmission of DTMF Tones According to RFC2833....414
11.2.3 Quality of Service....415
11.2.3.1 How to Configure Quality of Service (QoS)....417
11.3 IP Stations....417
11.4 SIP Stations....418
11.5 UP0 stations....421
11.6 DECT stations....421
11.7 Mitel SIP DECT stations....422
11.8 ISDN Stations....423
11.8.1 How to Configure the S_0 Interface for ISDN Stations....424
11.8.2 How to Allow only Configured Numbers for MSNs....425
11.9 Analog Stations....425
11.10 Virtual Stations....427
11.11 Key programming....427
11.11.1 How to Program the Function Keys on the System Phones....428
11.12 Station Profiles....429
11.13 Configuring Stations....429
11.13.1 How to Configure IP Stations....431

11.13.2 How to Configure SIP Stations....434
11.13.3 How to Configure UP0 Stations....438
11.13.4 How to Configure DECT Stations....441
11.13.5 How to Configure Mitel SIP DECT Stations through Provisioning....444
11.13.5.1 How to Configure SIP Stations via Expert Mode....446
11.13.6 How to Configure ISDN Stations....447
11.13.7 How to Configure Analog Stations....449
11.13.8 How to Edit Station Names....452
11.14 Configuring Station Profiles....453
11.14.1 How to Create a New Station Profile....453
11.14.2 How to Display Station Profiles and their Members....454
11.14.3 How to Add Members to a Station Profile....455
11.14.4 How to Delete Members from a Station Profile....455
11.14.5 How to Export or Import a Single Station Profile....456
11.14.6 How to Change Values and Settings of a Station Profile....457
11.14.7 How to Export or Import all Station Profiles....458
11.15 Configuring the Authentication Data at the SIP Phone....458
11.15.1 How to Configure the Authentication Data via the WBM of the SIP Phone....459
11.15.2 How to Configure the Authentication Data on the Display of the SIP Phone....461
11.16 Exporting Subscriber Data....462
11.16.1 How to Export the Station Data....463

12 UC Smart....464
12.1 Basic Settings for UC Smart....465
12.1.1 How to Activate UC Smart....465
12.1.2 How to Configure UC Smart....466
12.1.3 How to Configure Application-controlled Conferences....467
12.1.4 How to Determine the IP Addresses of the System Components....468
12.1.5 How to Determine the Status of C Smart....468
12.2 UC Smart Clients....468
12.2.1 myPortal @work....469
12.2.1.1 Prerequisites for myPortal @work....471
12.2.1.2 myPortal @work user configuration....472
12.2.1.3 Configuration steps to use myPortal @work via the internet....479
12.2.1.4 Other Configuration Hints & Settings....481
12.2.1.5 Troubleshooting Guide....483
12.2.1.6 Further Hints....484
12.3 Users of UC Smart....485
12.3.1 How to Configure UC Smart Users....486
12.3.2 How to Change the Password for a UC Smart User....486
12.4 Presence Status (Presence)....487
12.5 Directories and Journal....487
12.5.1 Directories....487
12.5.1.1 How to Configure Directories for System Telephones....488
12.5.2 Internal Directory....489
12.5.2.1 How to Enable or Disable the Display of Stations in the Internal Directory....489
12.5.3 Favorites List....490
12.5.4 System Directory....490
12.5.5 Unified Directory....490
12.5.5.1 Features....491
12.5.5.2 Rules and Conventions....494
12.5.5.3 Functional Boundaries....495
12.5.5.4 Unified Directory in Networked Systems....496
12.5.6 Journal....497
12.6 Calls....497
12.6.1 Call Number Formats....497

12.6.2 Prerequisites for receiving VoIP calls on myPortal to go using CallKit on your iPhone..... 498
12.7 Conferences..... 498
12.8 Web Collaboration..... 500
12.8.1 How to Configure the Connection to the Web Collaboration Server (Public Server)..... 501
12.8.2 How to Disable the Connection to the Web Collaboration Server..... 501
12.9 Instant Messaging..... 502
12.9.1 Instant Messaging..... 502
12.10 Voicemail Box (SmartVM)..... 502
12.10.1 Configuring the Voicemail Box (SmartVM)..... 504
12.10.1.1 How to Disable or Enable the Voicemail Box..... 505
12.10.1.2 How to Configure the Voicemail Box (SmartVM)..... 506
12.10.1.3 How to Add a Standard Voicemail Box for a Subscriber..... 507
12.10.1.4 How to Change the COS Group for a Voicemail Box Port..... 507
12.10.1.5 How to Change the Structure of the Phone Menu for the Voicemail Box..... 508
12.10.1.6 How to Load, Save and Delete Individual Greetings..... 508
12.10.1.7 How to Back up and Restore Greetings and Messages..... 509
12.10.2 Notification Service for Messages..... 510
12.10.2.1 How to Enable or Disable E-mail Notifications..... 510

13 UC Suite..... 512
13.1 Basic Settings for UC Suite..... 512
13.1.1 How to Activate UC Suite..... 512
13.1.2 How to Restrict the Authorization for UC Calls Initiated by the System..... 513
13.2 UC Suite Clients..... 513
13.2.1 myPortal for Desktop..... 514
13.2.2 myPortal @work..... 514
13.2.3 myPortal for Outlook..... 515
13.2.4 Fax Printer..... 515
13.2.5 myAttendant..... 515
13.2.6 Prerequisites for UC Suite PC Clients..... 516
13.2.7 Silent Installation/Uninstallation for UC Suite PC Clients..... 519
13.2.7.1 How to Perform a Silent Installation..... 520
13.2.7.2 How to Perform a Silent Uninstallation..... 521
13.2.8 Automatic Updates..... 522
13.3 Users and User Profiles of the UC Suite..... 523
13.3.1 Users of UC Suite..... 523
13.3.1.1 How to Configure UC Suite Users..... 525
13.3.1.2 How to Reset UC Suite Users..... 526
13.3.1.3 How to Configure UC Suite Users as Agents (myAgent)..... 526
13.3.1.4 How to Change the Presence Status for a UC Suite User..... 527
13.3.1.5 How to Change the Password for a UC Suite User..... 527
13.3.1.6 How to Change the Password Length for UC Suite Users..... 527
13.3.2 User Profiles for the UC Suite..... 528
13.3.2.1 How to Add a UC Suite User Profile..... 529
13.3.2.2 How to Edit a User Profile of the UC Suite..... 530
13.3.2.3 How to Display the User Profiles of the UC Suite..... 530
13.3.2.4 How to Add Members to a UC Suite User Profile..... 530
13.3.2.5 How to Delete Members from a UC Suite User Profile..... 531
13.3.2.6 How to Delete a UC Suite User Profile..... 531
13.4 Presence Status and CallMe Service..... 531
13.4.1 Presence Status (Presence)..... 532
13.4.2 CallMe Service..... 534
13.4.3 Status-based Call Forwarding..... 535
13.4.4 Rule-Based Call Forwarding..... 535
13.5 Directories and Journal..... 536
13.5.1 Directories..... 536

13.5.1.1 How to Configure Directories for System Telephones....538
13.5.2 Internal Directory....539
13.5.2.1 How to Enable or Disable the Display of Analog Stations in the Internal Directory....539
13.5.2.2 How to Enable or Disable Searching the Internal Directory only....540
13.5.3 External Directory....541
13.5.3.1 How to Import a CSV File from the Local File System into the External Directory....542
13.5.3.2 How to Add Access to an External Database for the External Directory....543
13.5.3.3 How to Export a CSV file from the External Directory....544
13.5.4 External Offline Directory (LDAP)....544
13.5.4.1 How to Add the External Offline Directory (LDAP) for PC Clients....545
13.5.4.2 How to Delete the External Offline Directory (LDAP) for PC Clients....546
13.5.4.3 How to Add an External Offline Directory (LDAP) for System Telephones....546
13.5.5 System Directory....547
13.5.6 Unified Directory....547
13.5.6.1 Features....548
13.5.6.2 Rules and Conventions....551
13.5.6.3 Functional Boundaries....552
13.5.6.4 Unified Directory in Networked Systems....553
13.5.6.5 How to Import Contacts to Unified Directory....554
13.5.6.6 How to Edit or Add new Unified Directory Contacts....555
13.5.7 Departments....555
13.5.7.1 How to Add a Department....556
13.5.7.2 How to Assign Stations to a Department....556
13.5.7.3 How to Edit a Department....556
13.5.7.4 How to Remove a Department....557
13.5.8 Favorites List....557
13.5.9 Journal....557
13.5.9.1 How to Change the Maximum Retention Period for the Journal....559
13.6 Calls....559
13.6.1 Desktop Dialer and Clipboard Dialer....559
13.6.2 Screen Pops....560
13.6.3 Record calls....560
13.6.3.1 How to Activate or Deactivate the Recording of Calls....561
13.6.3.2 How to Activate or Deactivate the Recording Announcement....561
13.6.3.3 How to Activate or Deactivate the Warning Tone for Recording....561
13.7 Conferences....562
13.7.1 Conference Management....562
13.7.1.1 How to Change the Dial-in Number for a Virtual Conference Room....566
13.7.1.2 Allowing or Preventing Multiple External Conference Participants....566
13.7.1.3 How to Activate or Deactivate the Conference Tone....567
13.7.1.4 How to Change the Time Interval for the Automatic Termination of a Conference....567
13.7.1.5 How to Check the Details of a Saved Conference....567
13.7.1.6 How to Delete a Saved Conference....568
13.7.1.7 How to Configure the Recording of Conferences....568
13.7.2 Ad-hoc Conference....568
13.7.3 Scheduled Conference....569
13.7.4 Permanent Conference....571
13.7.5 Open Conference....572
13.8 Web Collaboration....572
13.8.1 How to Configure the Connection to the Web Collaboration Server (Custom Server)....574
13.8.2 How to Configure the Connection to the Web Collaboration Server (Public Server)....575
13.8.3 How to Disable the Connection to the Web Collaboration Server....575
13.9 Instant Messaging....576
13.9.1 Instant Messaging....576
13.9.1.1 How to Enable or Disable Instant Messaging....577
13.10 AutoAttendant....577

13.10.1 Personal AutoAttendant ... 577
13.11 Voice and fax messages ... 578
13.11.1 Voicemail Box ... 578
13.11.1.1 How to Configure Station Numbers for Voicemail ... 580
13.11.1.2 How to Configure Call Forwarding to a Voicemail Box ... 580
13.11.1.3 How to Configure the Parameters of the Voicemail Box ... 580
13.11.1.4 How to Configure Retention Periods for Voicemail ... 581
13.11.1.5 How to Activate or Deactivate the Password Prompt for the Voicemail Box ... 581
13.11.1.6 How to Configure an Info for Received Voicemails ... 582
13.11.1.7 How to Configure a Mailbox Key to Check Voicemail ... 582
13.11.2 Voicemail Announcements ... 582
13.11.2.1 How to Import Announcements for the Voicemail Box ... 584
13.11.2.2 How to Change the Language for Voicemail Announcements ... 585
13.11.3 Fax Box ... 585
13.11.3.1 How to Add a Fax Box for Stations ... 586
13.11.3.2 How to Configure the File Type for Stored Fax Messages (UC Suite) ... 586
13.11.4 Sending Fax Messages with Fax Printer ... 586
13.11.4.1 How to Add a Central Cover Page ... 587
13.11.4.2 How to Edit a Central Cover Page ... 588
13.11.4.3 How to Add a Header Line for the Fax Printer ... 588
13.11.4.4 How to Edit a Header Line for Fax Printer ... 588
13.11.4.5 How to Delete a Header Line for Fax Printer ... 589
13.11.5 Notification Service for New Messages (UC Suite) ... 589
13.11.6 Sending E-mails ... 590
13.11.6.1 How to Configure the Sending of E-mails ... 590
13.11.7 SMS Template ... 591
13.11.7.1 How to Add an SMS Template ... 592
13.11.7.2 How to Edit an SMS Template ... 593
13.11.7.3 How to Remove an SMS Template ... 593
13.11.8 Fax over IP (T.38 / G.711 Fax) ... 594
13.11.8.1 How Enable or Disable Fax over IP (T.38 Fax) ... 595
13.12 Microsoft Office 365 Integration Overview ... 595
13.12.1 How to connect OpenScape Business system to Microsoft Office 365 using Basic Authentication ... 596
13.12.2 How to connect OpenScape Business system to Microsoft Office 365 using Modern Authentication ... 601
13.12.3 How to check that Microsoft Office 365 Integration features are configured ... 601

14 Functions at the Telephone ... 603
14.1 Making Call ... 603
14.1.1 Digit Dialing ... 603
14.1.2 En-Bloc Dialing ... 603
14.1.3 Keypad dial ... 603
14.1.4 End-of-Dialing Recognition ... 604
14.1.5 Editing the Telephone Number ... 604
14.1.5.1 How to Activate or Deactivate Editing of the Telephone Number ... 605
14.1.6 Redialing ... 605
14.1.6.1 How to Enable or Disable Automatic Redialing ... 606
14.1.7 System Speed Dialing ... 606
14.1.7.1 How to Add a Speed Dial ... 607
14.1.7.2 How to Import Speed Dials from an XML File ... 608
14.1.7.3 How to Export Speed Dials to an XML File ... 608
14.1.7.4 How to Edit Speed Dials ... 609
14.1.8 Individual Speed Dialing (ISD) ... 609
14.1.9 Direct station select ... 610
14.1.10 Speaker Calls / Direct Answering ... 610

14.1.10.1 How to Enable or Disable the Prevention of Speaker Calls for Stations....611
14.1.11 Associated Dialing....612
14.1.12 Trunk Queuing....612
14.1.12.1 How to Activate or Deactivate Trunk Queuing....612
14.1.13 Private Trunk....613
14.2 Call Signaling, Calling Line ID....613
14.2.1 Different Call Signaling....613
14.2.2 Calling Line Identification Presentation (CLIP)....614
14.2.2.1 How to Enable or Disable Configurable CLIP....614
14.2.3 Calling Line Identification Restriction (CLIR)....615
14.2.3.1 How to Enable or Disable Station Number Suppression....615
14.2.4 Connected Line Identification Presentation (COLP)....616
14.2.4.1 How to Enable or Disable Connected Line Identification Presentation (COLP)....616
14.2.5 Connected Line Identification Restriction (COLR)....616
14.2.6 CLIP No Screening (Transmission of Customer-Specific Phone Number Information)....616
14.2.6.1 How to Configure CLIP No Screening....617
14.2.7 CLIP for Analog Telephones....617
14.2.8 Ringer Cutoff....618
14.2.9 Translating Station Numbers to Names for System Speed Dialing....618
14.3 Functions During the Call....618
14.3.1 Placing a Call on Hold....618
14.3.2 Parking....618
14.3.3 Consultation....619
14.3.4 Toggle/Connect....620
14.3.5 Transfer....620
14.3.6 Automatic Recall....621
14.3.7 Call Supervision....622
14.3.7.1 How to Activate or Deactivate Call Supervision for a Station....622
14.3.8 Discreet Call (Whisper)....623
14.3.9 Live Call Recording (Voice Recording)....624
14.4 Controlling Availability....625
14.4.1 Call Forwarding....626
14.4.1.1 How to Configure Call Forwarding....627
14.4.2 Call Forwarding (CF)....629
14.4.2.1 How to Enable or Disable Call Forwarding over Analog Trunks....630
14.4.2.2 How to Enable or Disable Call Forwarding to the External Destination....630
14.4.3 Call Forwarding After Timeout....631
14.4.4 External Call Forwarding - No Answer (Not for U.S.)....631
14.4.5 Ringing Assignment / Call Allocation....632
14.4.5.1 How to How to Configure a Ringing Assignment....632
14.4.6 Ringing group on....632
14.4.7 Rejecting Calls....634
14.4.8 Deferring a Call....634
14.4.9 Do Not Disturb....634
14.5 Optimizing Communication....635
14.5.1 Callback....635
14.5.2 Call Waiting....636
14.5.2.1 How to Enable or Disable Call Waiting....637
14.5.2.2 How to Enable or Disable Immediate Call Waiting (Camp On) by the Attendant Console....637
14.5.3 Override (Intrusion)....638
14.5.3.1 How to Authorize an Internal Station for the Override Feature....639
14.5.3.2 How to Authorize the Intercept Position for the Override Feature....639
14.5.4 Advisory Messages....639
14.5.4.1 How to Edit Advisory Messages....640
14.5.5 Message Texts....640
14.5.5.1 How to Change a Message Text....640

14.5.6 Associated Services....641
14.5.6.1 How to Activate or Deactivate Associated Services....641
14.5.7 DISA....642
14.5.7.1 How to Activate or Deactivate a DISA Class of Service for a Station....642
14.5.7.2 How to Configure a DISA Number....643
14.5.7.3 How to Configure the DISA Security Mode....643
14.5.8 Flex Call/Mobile PIN....643
14.5.9 Relocate....644
14.5.9.1 How to Unlock Relocate on a System-wide Basis....644
14.5.10 Reset activated features....645
14.5.11 Procedures....645
14.5.12 Automatic Wake-up System and Timed Reminders....647
14.6 Overview of functions and codes....647

15 Working in a Team (Groups)....651
15.1 Call Pickup Group, Group Call and Hunt Group....651
15.1.1 Call Pickup Group....651
15.1.2 Group Call....653
15.1.3 Hunt Group....656
15.1.4 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Wizards....659
15.1.4.1 How to Configure a Call Pickup Group....660
15.1.4.2 How to Add or Delete a Member to or from a Call Pickup Group....660
15.1.4.3 How to Add a Group Call (Group)....661
15.1.4.4 How to Edit a Group Call (Group)....662
15.1.4.5 How to Delete a Group Call (Group)....663
15.1.4.6 How to Add or Delete a Member to or from a Group Call (Group)....664
15.1.4.7 How to Add a Hunt Group....664
15.1.4.8 How to Change a Hunt Group....665
15.1.4.9 How to Delete a Hunt Group....666
15.1.4.10 How to Add or Delete a Member to or from a Hunt Group....667
15.1.5 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Expert Mode....667
15.1.5.1 How to Enable or Disable the Display of a Caller's Station Number and Name....668
15.1.5.2 How to Activate or Deactivate the Warning Tone....668
15.1.5.3 How to Enable or Disable Call Pickup for Recalls....668
15.1.5.4 How to Add a Group Call (RNA or Call Waiting)....669
15.1.5.5 How to Display or Edit a Group Call (RNA or Call waiting)....670
15.1.5.6 How to Delete a Group Call (RNA or Call Waiting)....670
15.1.5.7 How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting)....670
15.1.5.8 How to Enable or Disable Do Not Disturb for a Group Member....671
15.2 Team Configuration / Team Group and Executive/Secretary / Top Group....671
15.2.1 Team Configuration / Team Group....672
15.2.2 Executive/Secretary or Top Group....676
15.2.3 Configuring Team Configurations / Team Groups and Executive/Secretary Functions / Top Groups using Wizards....680
15.2.3.1 How to Add a Team Configuration / Team Group....680
15.2.3.2 How to Edit a Team Configuration / Team Group....681
15.2.3.3 How to Delete a Team Configuration / Team Group....682
15.2.3.4 How to Add an Executive/Secretary or Top Group....683
15.2.3.5 How to Edit an Executive/Secretary or Top Group....684
15.2.3.6 How to Delete an Executive / Secretary or Top Group....685
15.2.4 Configuring Team configurations / Team groups and Executive/Secretary functions / Top groups using Expert mode....685
15.2.4.1 How to Add or Delete a Member to or from a Team Configuration or Team Group....686
15.2.4.2 How to Edit a Member of a Team Configuration / Team Group....686
15.2.4.3 How to Edit the Properties of Members in a Team Group....687
15.2.4.4 How to Change the Programmed Feature Keys for a Team Configuration / Team Group....687

15.2.4.5 How to Add a Fax Box to a Team Configuration / Team Group....688
15.2.4.6 How to Add or Delete a Member to or from an Executive/Secretary or Top Group....688
15.2.4.7 How to Edit a Member of an Executive/Secretary or Top Group....689
15.2.4.8 How to Edit the Properties of an Executive/Secretary or Top Group....689
15.2.4.9 How to Add a Fax Box to an Executive/Secretary or Top Group....690
15.3 Basic MULAP and Executive MULAP....690
15.3.1 Basic MULAP....690
15.3.2 Executive MULAP....693
15.3.3 Configuring Basic MULAPs and Executive MULAPs....695
15.3.3.1 How to Add a Basic MULAP....696
15.3.3.2 How to Display or Edit a Basic MULAP....696
15.3.3.3 How to Delete a Basic MULAP....697
15.3.3.4 How to Add or Delete a Member to or from a Basic MULAP....697
15.3.3.5 How to Edit a Member of a Basic MULAP....698
15.3.3.6 How to Add an Executive MULAP....698
15.3.3.7 How to Display or Edit an Executive MULAP....699
15.3.3.8 How to Delete an Executive MULAP....699
15.3.3.9 How to Add or Delete a Member to or from an Executive MULAP....699
15.3.3.10 How to Edit a Member of an Executive MULAP....700
15.3.3.11 How to Add a Basic MULAP in a Group....700
15.4 Voicemail Group and Fax Box Group....701
15.4.1 Voicemail Group....701
15.4.2 Fax Box Group....702
15.4.3 Configuring Voicemail Box Groups and Fax Box Groups....702
15.4.3.1 How to Add a Voicemail Group....703
15.4.3.2 How to Display or Edit a Voicemail Group....703
15.4.3.3 How to Delete a Voicemail Group....704
15.4.3.4 How to Add or Delete a Member to a Voicemail Group....704
15.4.3.5 How to Edit a Member of a Voicemail Group....704
15.4.3.6 How to Configure a Fax Box Group....705
15.4.3.7 How to Display or Edit a Fax Box Group....706
15.4.3.8 How to Delete a Fax Box Group....706
15.4.3.9 How to Add or Delete a Member to a Fax Box Group....706
15.5 Speaker Call for Groups....707
15.5.1 Internal Paging....707
15.5.2 Transfer to Group from Announcement....707
15.6 UCD (Uniform Call Distribution)....708
15.6.1 Call Distribution / UCD Group....708
15.6.1.1 How to Configure Call Distribution / UCD Groups....709
15.6.2 UCD Agents....710
15.6.2.1 How to Add or Delete UCD Agents....712
15.6.3 Wrap up....712
15.6.3.1 How to Change the Automatic Wrap-Up Time....713
15.6.4 Call Prioritization....713
15.6.4.1 How to Change Request Priorities....714
15.6.5 Accepting UCD Calls Automatically....714
15.6.5.1 How to Change the Automatic Acceptance of UCD Calls....714
15.6.6 UCD queue....715
15.6.6.1 How to Change the UCD Queue....715
15.6.7 UCD Overflow....716
15.6.7.1 How to Change the UCD Overflow....717
15.6.8 UCD Night Service....717
15.6.9 Announcements / Music on Hold for UCD....718
15.6.9.1 How to Change Announcements / Music on Hold for UCD....718
15.6.10 Transfer to UCD Groups....719
15.6.10.1 How to Edit the Recall Time for Calls Transferred to UCD Groups....719

15.6.11 Releasing UCD from Analog Lines....720
15.6.11.1 How to Edit the Release Time for UCD Calls over Analog Trunks....720

16 Call Routing....721
16.1 Classes of Service (Toll Restriction)....721
16.1.1 Class of Service (COS) Groups and Classes of Service....721
16.1.1.1 How to Edit COS Group Names....722
16.1.1.2 How to Edit the Classes of Service of a COS Group....722
16.1.1.3 How to Display All Stations of a COS Group....723
16.1.2 Allowed and Denied Lists....723
16.1.2.1 How to Create a List of Emergency Numbers....724
16.1.2.2 How to Create an Allowed and a Denied List....724
16.1.2.3 How to Create Additional Allowed Lists....725
16.1.2.4 How to Create Additional Denied Lists....725
16.1.2.5 How to Display all Call Numbers in a Denied List....726
16.1.2.6 How to Display all Call Numbers in an Allowed List....726
16.1.2.7 How to Edit the Analysis Filter for the Denied List....726
16.1.3 Blacklist....727
16.1.3.1 How to Create a Blacklist for incoming calls in Expert mode....727
16.1.3.2 How to Edit/Delete Call Numbers in the Blacklist....728
16.1.3.3 How to Display Call Numbers in the Blacklist....729
16.1.3.4 How to Create a Blacklist for incoming calls in Setup....729
16.1.4 Night Service....730
16.1.4.1 How to Assign Classes of Service for the (Manual) Night Service....731
16.1.4.2 How to Delete Classes of Service for the Manual Night Service....731
16.1.4.3 How to Configure the Scheduled Night Service....732
16.1.4.4 How to Configure a Special Day for the Scheduled Night Service....732
16.1.4.5 How to Delete a Special Day for the Scheduled Night Service....732
16.1.5 Automatic COS Changeover after Time....733
16.1.5.1 Schedule....733
16.1.6 CON Groups....734
16.1.6.1 CON groups (traffic restriction groups)....735
16.1.6.2 Assigning Speed-Dialing Numbers to CON groups....735
16.1.6.3 How to Assign Stations to a CON Group....736
16.1.6.4 How to Assign a Trunk to a CON Group....736
16.1.6.5 How to Edit the CON Matrix....736
16.1.7 System Telephone Lock (COS Changeover)....737
16.1.8 Individual Lock Code (Locking the Phone)....737
16.1.8.1 How to Reset the Individual Lock Code....738
16.1.9 Collect Call Barring per Trunk (for Brazil only)....738
16.1.10 Ringback Protection per Station (for Brazil only)....738
16.2 LCR (Least Cost Routing)....738
16.2.1 LCR Functionality....739
16.2.1.1 How to Release LCR....741
16.2.2 LCR Dial Plan....742
16.2.2.1 How to Edit the Dial Plan....743
16.2.3 LCR Routing Table....743
16.2.3.1 How to Edit Routing Tables....744
16.2.4 LCR Class of Service....745
16.2.4.1 How to Assign and Change an LCR Class of Service....745
16.2.5 LCR Outdial Rules....746
16.2.5.1 How to Edit the Outdial Rules....747
16.2.6 Network carriers....748
16.2.7 Selective Seizure of Exchange Lines....749
16.2.7.1 How to Configure the Code for the Selective Seizure of ISDN Trunks....749
16.2.7.2 How to Display the Seizure Code for the 'Outside Line Seizure'....750

16.3 Digit Analysis and Call Routing....750
16.3.1 Overview of Call Routing / LCR....751
16.3.2 Digit Analysis Flowchart....754
16.3.3 Call Routing and LCR in the Internetwork....755
16.3.3.1 Dedicated Gateway....757
16.3.4 Scenarios: Digit Analysis and Call Routing....758
16.3.4.1 Subscriber A Calls Subscriber B via an Internal Phone Number....759
16.3.4.2 Subscriber A calls subscriber B via a public phone number....759
16.3.4.3 Subscriber A calls an external station via the CO....760
16.3.4.4 ISDN trunk calls subscriber A....761
16.3.4.5 Special Configurations....762
16.3.4.6 Subscriber A Calls Subscriber C via an Internal Phone Number....763
16.3.4.7 Subscriber A calls subscriber C via a public number in the internetwork....764
16.3.4.8 ISDN trunk calls subscriber C....767
16.3.4.9 ISDN Trunk Gateway 1 Calls Subscriber D....768
16.3.4.10 Subscriber D calls external station via the CO....771
16.4 Emergency Calls....773
16.4.1 Hotline after Timeout / Hotline....774
16.4.1.1 How to Configure and Change the Hotline Destination....775
16.4.1.2 How to Change the Hotline Timeout....775
16.4.1.3 How to Configure an Off-Hook Alarm after Timeout or Hotline for a Station....775
16.4.2 Trunk Release for Emergency Call....776
16.4.2.1 How to Activate and Deactivate Trunk Release for Emergency Call....776
16.4.3 For U.S. and Canada only: E911 Emergency Call Service....777
16.4.3.1 How to Edit CLIP / Lin....777
16.4.4 Emergency Calls in Combination with Mobile Logon....777
16.4.4.1 Configuring the Emergency Scenario....778
16.4.5 E112 Emergency Call Service for Europe....780
16.4.5.1 How to add ITSP-Loc ID to a station....781
16.5 Call Admission Control....781
16.5.1 Limiting the Number of Simultaneous Calls via an ITSP....781
16.5.2 Restricting the bandwidth requirements for gateway calls....782
16.5.3 Limiting the Number of Calls in Networking Scenarios....782
16.6 Tenant system....782
16.6.1 System Speed Dialing in Tenant Systems....784

17 Attendants....785
17.1 AutoAttendant....785
17.1.1 Company AutoAttendant (UC Smart)....787
17.1.1.1 How to Configure an Established Company AutoAttendant....788
17.1.1.2 How to Set up a New Company AutoAttendant....789
17.1.2 Company AutoAttendant (UC Suite)....790
17.1.2.1 Schedules....791
17.1.2.2 Templates....799
17.2 OpenStage Attendant....801
17.3 OpenScape Business Attendant....801
17.3.1 OpenScape Business BLF....804
17.3.2 Configuration Examples for OpenScape Business Attendant, OpenScape Business BLF....804
17.3.2.1 Scenario 1: OpenScape Business Attendant Connected to an OpenScape Business Single System....805
17.3.2.2 Scenario 2: Two or More OpenScape Business Attendants Connected to an OpenScape Business Single System....810
17.3.2.3 Scenario 3: OpenScape Business Network with Individual OpenScape Business Attendants (Network-wide BLF and Presence Status via WSI)....812
17.3.2.4 Scenario 4: OpenScape Business Network with central OpenScape Business Attendant (Network-wide BLF and Presence Status via WSI)....812

17.3.2.5 Scenario 5: OpenScape Business BLF Connected to an OpenScape Business Single System....813
17.3.2.6 Scenario 6: OpenScape Business BLF Connected to an OpenScape Business Internetwork (BLF and Presence Status via WSI)....815
17.4 myAttendant....815
17.4.1 Subscriber Management....817
17.4.2 Message Center....817
17.4.3 Scenario 1: How to Configure a myAttendant connected to an OpenScape Business Single System....818
17.4.4 Scenario 2: How to Configure Two or More myAttendants connected to an OpenScape Business Single System....819
17.4.5 Scenario 3: How to Set Up an OpenScape Business Network with a Central myAttendant....820
17.5 Intercept Position....821
17.5.1 How to Configure the Intercept Position and Intercept Criteria....823
17.5.2 How to Configure the Central Intercept Position....823
17.5.3 How to Configure the Telephone Lock Intercept....824
17.5.4 How to Configure the Intercept Announcement....824

18 Multimedia Contact Center....825
18.1 Contact Center Clients....825
18.1.1 myAgent....825
18.1.2 Prerequisites for myAgent....827
18.1.3 myReports....829
18.1.3.1 How to Reset the myReports Administrator Password....830
18.1.4 Prerequisites for myReports....830
18.1.5 Notes on Using myAgent and UC Suite Clients Simultaneously....832
18.2 Agents....833
18.2.1 Agent Functions Independent of the Authorization Level....834
18.2.2 Preferred Agents....835
18.2.3 Agents in multiple queues....835
18.2.4 Contact Center Breaks....835
18.2.5 Agent Login/Logout via Telephone....835
18.3 Queues and Schedules....838
18.3.1 Queues....838
18.3.2 Schedules....840
18.3.3 Wrap up....847
18.3.4 Grade of Service....848
18.3.5 Wallboard....848
18.3.6 Agent Callback....849
18.4 VIP service....849
18.4.1 VIP Caller Priority....849
18.4.2 VIP Call List....849
18.5 Fallback solution....850
18.6 Configuring the Contact Center....853
18.6.1 Example of a Contact Center Configuration....853
18.6.1.1 How to Configure UCD Groups for the Sample Contact Center....855
18.6.1.2 How to Configure a Fallback Solution for the Sample Contact Center....856
18.6.1.3 How to Configure a Subscriber as an Agent for the Sample Contact Center....857
18.6.1.4 How to Add Announcements for the Sample Contact Center....857
18.6.1.5 How to Load Announcements for the Sample Contact Center....858
18.6.1.6 How to Add the Standard Schedule XYZ for the Sample Contact Center....859
18.6.1.7 How to Add the Standard Schedule Hotline for the Sample Contact Center....863
18.6.1.8 How to Add Queues for the Sample Contact Center....865
18.6.1.9 How to Assign Agents to Queues of the Sample Contact Center....867
18.6.2 Configuration Procedure....868
18.6.2.1 How to Configure UCD Groups for the Contact Center....869

18.6.2.2 How to Configure a Subscriber as an Agent....869
18.6.2.3 How to Record Custom Announcements for the Contact Center....870
18.6.2.4 How to Load Custom Announcements for the Contact Center....871
18.6.2.5 How to Add a Schedule....871
18.6.2.6 How to Edit a Schedule....874
18.6.2.7 How to Delete a Schedule....875
18.6.2.8 How to Save a Rule (CCV) as a PDF File....876
18.6.2.9 How to Download a Rule (CCV) as a Backup File....876
18.6.2.10 How to Upload a Downloaded Rule (CCV) in a Backup File Format....877
18.6.2.11 How to Add a Queue....877
18.6.2.12 How to Edit a Queue....881
18.6.2.13 How to Activate or Deactivate a Queue....883
18.6.2.14 How to Configure a Pilot for Incoming Fax Messages in Queues....883
18.6.2.15 How to Define Target Values for the Grade Of Service....884
18.6.2.16 How to Define the VIP Caller Priority....884
18.6.2.17 How to Edit the VIP Call List....885
18.6.2.18 How to Define Preferred Agents....886
18.6.2.19 How to Delete Preferred Agents....886
18.6.2.20 How to Add a Contact Center Break....886
18.6.2.21 How to Edit a Contact Center Break....887
18.6.2.22 How to Delete a Contact Center Break....887
18.6.2.23 How to Add a Wrapup Reason for a "Simple Wrapup"....888
18.6.2.24 How to Edit a Wrapup Reason for a "Simple Wrapup"....888
18.6.2.25 How to Delete a Wrapup Reason for a "Simple Wrapup"....888
18.6.2.26 How to Add a Wrapup Reason for a "Multiple Wrapup"....889
18.6.2.27 How to Edit a Wrapup Reason for a "Multiple Wrapup"....889
18.6.2.28 How to Delete a Wrapup Reason for a "Multiple Wrapup"....890
18.6.2.29 How to Assign an Agent to a Queue....890
18.6.2.30 How to Remove an Agent from the Queue....891
18.7 Notes on Using the Contact Center....892
18.7.1 Restrictions on Operating the Contact Center....892
18.8 Notes on the Use of DECT Phones....894
18.9 Reports....895
18.9.1 Predefined Report Templates....896

19 Mobility....898
19.1 Integrated Mobility Solution....898
19.2 Mobility on the Road....898
19.2.1 myPortal to go....899
19.2.1.1 Prerequisites for myPortal to go....901
19.2.2 Mobility Entry....902
19.2.3 Comparison between Mobile Clients and Mobility Entry....904
19.2.4 Dependencies for Mobile Clients and Mobility Entry....906
19.2.5 One Number Service (ONS)....907
19.2.6 Dual-Mode Telephony....908
19.2.7 Configuring myPortal to go and Mobility Entry....908
19.2.7.1 How to Integrate GSM Mobile Phones....909
19.2.7.2 How to Integrate Dual-Mode Telephones (GSM/WLAN) with HFA or SIP Client....911
19.2.7.3 How to Enable the Web Interface for Mobile Phones and Web Clients....912
19.2.7.4 How to Delete Mobile Phone Integration....913
19.3 Mobility in the office....914
19.3.1 Desk Sharing....914
19.3.2 Integrated Cordless Solution....915
19.3.2.1 System Overview....916
19.3.2.2 System Configuration....917
19.3.2.3 Cordless/DECT Phones....918

19.3.2.4 Significance of Results Obtained from Testing the Radio Area....918
19.3.3 Configuring the Integrated Cordless Solution....921
19.3.3.1 How to Configure the DECT System ID and Other Cordless Parameters (System-wide Data)...921
19.3.3.2 How to Configure Cordless Base Stations....922
19.3.3.3 How to configure DECT Phones for the First Time....922
19.3.3.4 How to Register a DECT Phone (OpenStage/Gigaset Handset) at the Cordless System....923
19.3.3.5 How to Add Additional DECT Phones....925
19.3.3.6 How to Delete DECT Telephones....925
19.3.3.7 How to Configure the Multi-SLC Parameters....926
19.3.3.8 How to Query the Data for Base Stations....926
19.3.3.9 How to Enable the Message Waiting Indication (MWI) for DECT Telephones....927
19.3.3.10 How to Check the Logon Status of DECT Phones....927
19.3.4 Cordless IP....928
19.3.5 WLAN Phones and Access Points....928
19.3.5.1 WLAN Requirements....928
19.4 Mobility at Home....929
19.4.1 Configuring a VPN....930
19.4.2 Configuration for SIP Device@Home....930
19.4.3 Configuration for System Device@Home....932
19.4.4 How to Enable Device@Home....934
19.4.5 How to update software for System Device (HFA) @Home....935
19.4.6 How to Specify a STUN Server for Device@Home....937

20 Security....938
20.1 Firewall....938
20.1.1 Port Handling....938
20.1.1.1 Opening Ports....939
20.1.1.2 How to Configure the Opening of Ports....939
20.1.1.3 Port Management....940
20.1.1.4 How to Edit Global Port Management Settings....940
20.1.2 NAT....940
20.1.2.1 How to Configure a NAT Rule....941
20.1.2.2 How to Configure NAT Rules with the NAT Table Editor....942
20.1.2.3 How to Delete a NAT Rule....943
20.1.3 Application Firewall....943
20.1.3.1 How to Display the Configuration of the Application Firewall....944
20.1.3.2 How to Restrict Services using the Application Firewall....944
20.1.3.3 How to Delete the Configuration of the Application Firewall....945
20.1.4 Services Administration (OpenScape Business S)....945
20.1.4.1 How to Add or Block Services....945
20.2 Signaling and Payload Encryption (SPE)....946
20.2.1 How to Enable or Disable SPE Support....948
20.2.2 How Change the SPE Security Settings....948
20.2.3 How to Import an SPE Certificate and Private Key (PKCS#12)....948
20.2.4 How to Import an SPE CA Certificate....949
20.2.5 How to Enable or Disable SPE for a Station....949
20.3 Virtual Private Network (VPN)....950
20.3.1 Requirements for VPN....951
20.3.2 Connecting Teleworkers via a VPN....953
20.3.2.1 How to Connect Teleworkers via a VPN....954
20.3.2.2 How to Export Teleworker Data....955
20.3.3 Networking Communication Systems via a VPN....956
20.3.3.1 How to Configure Networking via a VPN....956
20.3.3.2 How to Import and Export the Topology Data of a VPN Network....958
20.3.4 VPN - Security Mechanisms....959
20.3.5 VPN - Certificates....961

20.3.5.1 VPN - How to Generate Lightweight CA Certificates....962
20.3.5.2 VPN - Certificate Management - How to View a Certificate....963
20.3.5.3 VPN - How to Import a Trusted CA Certificate (X.509)....963
20.3.5.4 VPN - Peer Certificates - How to Generate a Certificate Signing Request (CSR)....964
20.3.5.5 VPN - Peer Certificates - How to Generate a Certificate (PKCS#12)....964
20.3.5.6 VPN - How to Import a Peer Certificate (PKCS#12)....965
20.3.6 VPN Clients....966
20.3.6.1 NCP VPN Client Settings....967
20.3.6.2 How to Configure an NCP VPN Client....969
20.3.6.3 How to Configure a Shrew Soft VPN Client....969
20.3.6.4 How to Configure an iOS or Android VPN Client....970
20.3.6.5 How to Configure a Mac OS X VPN Client....970
20.3.7 VPN Services....971
20.3.7.1 VPN - Active Services - How to Display all IPsec Services....971
20.3.7.2 VPN - Active Services - How to Display a Special IPsec Service....972
20.3.7.3 VPN - Configured Services - How to Display all IPsec Services....972
20.3.7.4 VPN - Configured Services - How to Edit the IPsec Service....972
20.3.7.5 VPN - Configured Services - How to Rename the IPsec Service....973
20.3.7.6 VPN - Configured Services - How to Delete the IPsec Service....973
20.3.8 VPN tunnel....973
20.3.8.1 VPN - Active Tunnels - How to Display General Tunnel Data....974
20.3.8.2 VPN - Active Tunnels - How to Display Rules for all Tunnels....974
20.3.8.3 VPN - Configured Tunnels - How to Display General Tunnel Data....975
20.3.8.4 VPN - Configured Tunnels - How to Display Rules for all Tunnels....975
20.3.8.5 VPN - How to Add a Configured Tunnel....976
20.3.9 VPN rules....977
20.3.9.1 VPN - Active Rules - How to Display Rules....977
20.3.9.2 VPN - Active Rules - How to Display Special Rules....978
20.3.9.3 VPN - Configured Rules - How to Display all Rules....978
20.3.9.4 VPN - Configured Rules - How to Add a Rule....979
20.3.9.5 VPN - How to Edit a Rule....979
20.3.9.6 VPN - How to Add a Rule for the Opposite Direction....980
20.3.9.7 VPN - How to Delete a Rule....980
20.3.10 PKI Server....980
20.3.10.1 VPN - How to Display the PKI Server....981
20.3.10.2 VPN - How to Add a PKI Server....981
20.4 Certificate Handling....981
20.4.1 Introduction....982
20.4.2 How to Generate CA Certificates....983
20.4.3 How to Generate Self-Signed Certificates....984
20.4.4 How to Generate Certificate Signing Requests (CSR)....984
20.4.5 How to Import Server Certificates (PKCS#12)....986
20.4.6 How to Import Server Certificates (PEM)....986
20.4.7 How to Display Certificates....987
20.4.8 How to Delete Certificates....987
20.4.9 How to Export Certificates (X.509)....988
20.4.10 How to Import Updated Certificates (X.509)....988
20.4.11 How to Activate Certificates....988
20.4.12 Certificate Handling for Booster Server....989
20.5 Web Security....990
20.5.1 Connections to the Web Server....990
20.5.1.1 How to Configure Connections to the Web Server (UC Suite)....990
20.5.1.2 How to Configure Connections to the Web Server (UC Smart)....990
20.5.2 Admin Log (also called Admin Protocol)....991
20.5.2.1 How to Load the Admin Log....991
20.5.2.2 How to Change the Admin Log Language....991

20.6 SQL Security ... 992
20.6.1 Single node ... 992
20.6.2 Multinode ... 992
20.6.3 How to Configure Passwords to the SQL Database ... 993
20.7 SIP Attack Protection ... 994

21 Networking OpenScape Business ... 995
21.1 Network Plan ... 996
21.1.1 Homogeneous and Heterogeneous Networks ... 996
21.1.1.1 How to Display the Overview of all OpenScape Business Nodes ... 997
21.1.2 Single and Multi-Gateway ... 997
21.2 Network-wide Features ... 998
21.2.1 Network-wide Features of the UC Solutions ... 998
21.2.2 Network-wide Voice Features ... 1001
21.3 Licensing an Internetwork ... 1002
21.4 Networking Requirements ... 1002
21.4.1 LAN Networking Requirements ... 1003
21.4.2 Dial Plan in the Network ... 1005
21.4.2.1 Dialing Public Phone Numbers in the Network ... 1006
21.5 Path Optimization (Path Replacement) ... 1006
21.5.1 How to Enable or Disable Path Optimization (Path Replacement) ... 1007
21.6 Networking Scenarios ... 1007
21.6.1 Dependencies and Restrictions ... 1008
21.6.2 Networking Multiple OpenScape Business X Systems ... 1008
21.6.2.1 How to Configure the Basic Installation for Node 1 (Master) ... 1012
21.6.2.2 How to Configure Networking for Node 1 (Master) ... 1013
21.6.2.3 How to Configure the Basic Installation for Node 2 (Slave) ... 1014
21.6.2.4 How to Configure Networking for Node 2 (Slave) ... 1015
21.6.2.5 How to Verify the Networking Function for the Master ... 1015
21.6.2.6 How to Configure Routes and Routing Parameters (ISDN Trunk for the Master) ... 1016
21.6.2.7 How to Configure Routes and Routing Parameters (Trk. Grp. 16) (Master) ... 1016
21.6.2.8 How to Configure Least Cost Routing (LCR) for the Network (Master) ... 1017
21.6.2.9 How to Configure Routes and Routing Parameters (Slave) ... 1018
21.6.2.10 How to Configure Least Cost Routing (LCR) for the Network (Slave) ... 1019
21.6.3 Networking OpenScape Business X and OpenScape Business S (Single Gateway) ... 1020
21.6.3.1 How to Configure the Basic Installation for Node 1 (Master) ... 1025
21.6.3.2 How to Configure Networking for Node 1 (Master) ... 1026
21.6.3.3 How to Configure the Basic Installation for Node 2 (Slave) ... 1027
21.6.3.4 How to Configure Networking for Node 2 (Slave) ... 1028
21.6.3.5 How to Configure the Basic Installation for Node 3 (Slave) ... 1028
21.6.3.6 How to Verify the Networking Function for the Master ... 1029
21.6.3.7 Configure networking for node 3 (slave) ... 1030
21.6.3.8 How to Configure Least Cost Routing (LCR) for the Network (Node 3, Slave) ... 1030
21.6.3.9 How to Configure LCR for Networking (Node 2) ... 1032
21.6.3.10 How to Configure Routes and Routing Parameters (Node 1, Master) ... 1033
21.6.3.11 How to Configure Routes and Routing Parameters (Trk. Grp. 16, Node 1) ... 1034
21.6.3.12 How to Configure Least Cost Routing (LCR) for the Network (Node 1) ... 1034
21.6.4 Networking OpenScape Business X and OpenScape Business S (Multi-Gateway) ... 1036
21.6.4.1 How to Configure the Basic Installation for Node 4 (OpenScape Business S, Master) ... 1044
21.6.4.2 How to Configure the Networking for Node 4 (Master) ... 1045
21.6.4.3 How to Configure the Basic Installation for Node 1 (Slave) ... 1046
21.6.4.4 How to Configure Networking for Node 1 (Slave) ... 1047
21.6.4.5 How to Configure the Basic Installation for Node 2 (Slave) ... 1047
21.6.4.6 How to Configure Networking for Node 2 (Slave) ... 1048
21.6.4.7 How to Configure the Basic Installation for Node 3 (Slave) ... 1049
21.6.4.8 How to Configure Networking for Node 3 (Slave) ... 1049

21.6.4.9 How to Verify the Networking Function for the Master....1050
21.6.4.10 How to Configure a Multi-Gateway for Node 4 (Master)....1050
21.6.4.11 How to Configure Routes and Routing Parameters (Node 1, Slave)....1051
21.6.4.12 How to Configure Least Cost Routing (LCR) for the Network (Node 1, Slave)....1052
21.6.4.13 How to Configure Routes and Routing Parameters (Node 2, Slave)....1054
21.6.4.14 How to Configure Least Cost Routing (LCR) for the Network (Node 2, Slave)....1054
21.6.4.15 How to Configure Routes and Routing Parameters (Node 3, Slave)....1056
21.6.4.16 How to Configure Least Cost Routing (LCR) for the Network (Node 3, Slave)....1057
21.6.4.17 How to Configure Routes and Routing Parameters (Node 4, Master)....1059
21.6.4.18 How to Configure Least Cost Routing (LCR) for the Network (Node 4, Master)....1059
21.6.5 Networking OpenScape Business in Hosting Environments....1062
21.6.6 Networking OpenScape Business X and OpenScape 4000....1065
21.6.7 Networking OpenScape Business X and OpenScape Voice....1072
21.6.8 Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection....1075
21.6.9 Open Numbering in OpenScape Business X Networks....1077
21.6.9.1 How to Configure Open Numbering....1078
21.6.10 Networking via ISDN....1079
21.6.11 OpenScape Business internetwork with central ITSP trunk connection....1081
21.7 Central Intercept Position in the Internetwork (Not for U.S.)....1083
21.7.1 How to Configure a Central Intercept Position in the Multi-Gateway Internetwork....1084
21.8 Presence Manager....1085
21.9 Synchronization Status in the Internetwork....1086
21.9.1 Manual Synchronization in the Internetwork....1086
21.9.2 How to Start Synchronization Manually....1087
21.10 Survivability....1087
21.10.1 How to Configure Survivability....1090
21.11 Removing a Node from the Internetwork....1090

22 Auxiliary Equipment....1091
22.1 Analog Announcement Device....1091
22.1.1 How to Add an Analog Announcement Device....1092
22.1.2 How to Change the Announcement Delay Time....1093
22.2 Entrance Telephone and Door Opener....1093
22.2.1 DoorLine a/b T01-T04....1093
22.2.1.1 How to Configure the Station Port of the DoorLine a/b T01-T04....1094
22.2.1.2 How To Configure the Extension for the Doorline a/b T01-T04....1095
22.2.2 DoorCom Analog....1095
22.2.2.1 How to Configure the Station Port of the DoorCom Analog....1096
22.2.2.2 How to Configure DoorCom Analog Extensions....1096
22.2.3 Entrance Telephone with Amplifier (TFE-S)....1096
22.2.3.1 How to Configure the Entrance Telephone....1098
22.2.4 Loudspeakers....1098
22.2.4.1 How to Configure the Analog Station Interface for a Loudspeaker....1099
22.2.4.2 How to Configure the Analog Station Interface for Connecting an Amplifier to the TFE-S Module....1099
22.3 Relays....1100
22.3.1 How to Configure an Actuator....1102
22.4 Sensors....1102

23 Application Connectivity....1104
23.1 CSTA....1104
23.1.1 How to Change the Port Number for CSTA....1106
23.1.2 How to Enable or Disable the CMD for the Use of TAPI 120....1107
23.1.3 How to Enable or Disable the DSS Server for the Use of Network-Wide DSS Keys....1107
23.1.4 How to Activate or Deactivate the CSP....1108
23.1.5 How to Enable or Disable the Media Extension Bridge....1108

23.2 OpenScape Business TAPI 120/170....1108
23.2.1 OpenScape Business TAPI 120....1110
23.2.2 OpenScape Business TAPI 170....1114
23.3 Web Services Interface....1119
23.4 Open Directory Service....1120
23.4.1 How to Enable or Disable the Open Directory Service....1124
23.4.2 How to Restart the Open Directory Service....1125
23.4.3 How to Configure the Password for Access to the Open Directory Service....1125
23.4.4 How to Configure the ODBC to ODBC Bridge Server....1125
23.4.5 How to Add an External Data Source for the Open Directory Service....1127
23.4.6 How to Preview LDAP Search Results for the Open Directory Service....1130
23.4.7 How to Delete an External Data Source for the Open Directory Service....1130
23.5 Active Directory Integration Service....1131
23.5.1 How to Configure the Active Directory Service....1132
23.6 Application Launcher....1133
23.6.1 Prerequisites for Application Launcher....1133
23.6.2 Profile with Configuration Data for Application Launcher....1134
23.6.2.1 How to Provide a Profile with Configuration Data for Application Launcher....1135
23.7 myPortal for Teams overview....1135
23.7.1 How to configure myPortal for Teams....1136
23.7.2 How to upload myPortal for Teams to Teams store....1136
23.8 Unify Phone....1137
23.8.1 How to Configure the Unify Phone Connectivity....1137
23.8.2 How to configure the Unify Phone user instance....1139
23.8.3 How to Manage Unify Phone Users....1139
23.8.3.1 How to Create New Unify Phone Users....1139
23.8.3.2 How to Add Existing Unify Phone Users....1140
23.8.3.3 How to Edit Unify Phone User Details....1141
23.8.3.4 How to Remove or Delete Unify Phone Users....1141
23.8.3.5 How to prepare Alternative number and Call routing for Unify Phone interworking....1142
23.9 Let's Encrypt Service....1142
23.9.1 How to configure Let's Encrypt service....1143
23.10 CloudLink Service....1143
23.10.1 How to configure CloudLink service....1144
23.10.2 How to open the CloudLink Daemon web interface....1144
23.10.3 How to configure CloudLink Daemon web interface....1145
23.10.4 How to enable / configure SIP Connector to connect to Workflow Studio....1145
23.11 CloudLink Pilot Numbers....1146
23.11.1 How to configure CloudLink Pilot Numbers....1146

24 Accounting....1148
24.1 Connection Data....1148
24.1.1 Connection Data Recording....1148
24.1.1.1 How to Enable or Disable Connection Data Recording....1149
24.1.1.2 How to Activate or Deactivate Logging of the Connection Duration....1149
24.1.1.3 How to Configure the Logging of Currency Amounts or Call Charge Units....1149
24.1.1.4 How to Configure Call Charge Factors, Currency and Computing Accuracy....1150
24.1.1.5 How to Activate or Deactivate the Logging of the Last Four Digits....1150
24.1.1.6 How to Enable or Disable Outgoing Call Logging without a Connection....1151
24.1.1.7 How to Enable or Disable the Logging of Incoming Calls....1151
24.1.1.8 How to Activate or Deactivate the Connection Log....1152
24.1.1.9 How to Activate or Deactivate MSN Logging....1152
24.1.1.10 How to Activate or Deactivate the Decimal Format....1152
24.1.2 Account codes....1153
24.1.2.1 How to Configure Account Codes....1154
24.1.2.2 How to Configure an Account Code Checking Procedure....1154

24.1.2.3 How to Activate or Deactivate Number Redial with ACCT....1154
24.2 Displaying and Transmitting Connection Data....1155
24.2.1 Call-Charge Display with Currency (not for U.S.)....1155
24.2.1.1 How to Configure the Call-Charge Display with Currency....1156
24.2.2 Displaying the Connection Charges on the Phone....1156
24.2.3 Displaying the Connection Duration on the Phone....1156
24.2.3.1 How to Activate or Deactivate the Connection Duration Display....1157
24.2.4 Transmission of Connection Data....1157
24.2.4.1 How to Select the Format....1163
24.2.4.2 How to Enable or Disable Transmission of Connection Data via HTTPS....1164
24.3 Cost control....1164
24.3.1 Expensive Connection Route Advisory....1164
24.3.1.1 How to Configure an Expensive Connection Route Advisory....1165
24.3.2 Toll Fraud Monitoring....1165
24.3.2.1 How to Enable or Disable Toll Fraud Monitoring....1165
24.4 Accounting Tools....1166
24.4.1 Accounting Manager....1166
24.4.2 Teledata Office....1166

25 Maintenance....1167
25.1 Telephony Configuration....1167
25.1.1 Date and Time....1167
25.1.1.1 How to Configure the Date and Time Manually....1168
25.1.1.2 How to Set the Time Zone....1168
25.1.1.3 How to Configure the Date Format....1168
25.1.2 SNTP....1169
25.1.2.1 How to Obtain the Date and Time from an SNTP Server....1169
25.1.3 Telephone Logos....1169
25.1.3.1 How to Load a Phone Logo into the System....1170
25.1.3.2 How to Deploy a Phone Logo to System Telephones....1170
25.1.3.3 How to Delete a Phone Logo....1171
25.1.4 Customized Display....1171
25.1.4.1 How to Change the Customer-Specific Display (System Name)....1171
25.1.5 Multilingual Text Output....1172
25.1.6 Flexible Menus....1172
25.1.6.1 How to Edit the Flexible Menu....1172
25.1.7 Music on Hold....1173
25.1.7.1 How to Import Internal Music On Hold....1174
25.1.7.2 How to Configure the Music on Hold Functionality....1174
25.1.7.3 How to Change the Music on Hold Functionality for Each CON Group....1175
25.1.8 Announcements....1175
25.1.8.1 How to Configure Announcements (UC Suite & UC Booster)....1176
25.1.8.2 How to Configure Announcements (UC Smart)....1177
25.1.9 User to User Signaling....1178
25.1.10 Voice Channel Signaling Security....1178
25.1.11 Time Parameters....1178
25.1.12 Controlling Centrex Features....1178
25.1.12.1 How to Enable or Disable the Control of Centrex Features....1179
25.2 Backup and Restore....1179
25.2.1 Backup Sets....1180
25.2.1.1 How to Display Backup Sets....1181
25.2.1.2 How to Delete Backup Sets....1181
25.2.2 Backup Media....1181
25.2.2.1 How to Add a Backup Medium....1182
25.2.2.2 How to Edit a Backup Medium....1183
25.2.2.3 How to Delete a Backup Medium....1184

25.2.3 Immediate Backup....1184
25.2.3.1 How to Save a Backup Set Immediately....1185
25.2.4 Scheduled Backup....1186
25.2.4.1 How to Save a Backup Set with a Scheduled Backup....1186
25.2.5 Restore....1187
25.2.5.1 How to Restore a Backup Set....1187
25.3 Updates....1188
25.3.1 Using a Local Web Server....1189
25.3.1.1 How to Configure Access to the Local Web Server....1189
25.3.2 Updating the Communication System....1190
25.3.2.1 How to Update the System via a Web Server....1192
25.3.2.2 How to Update the System using a USB Storage Device....1193
25.3.2.3 How to Update the System via File Upload....1194
25.3.2.4 How to Update the System via a USB Device without WBM Access....1196
25.3.3 Updating System Telephones....1196
25.3.3.1 How to Load the Phone Software into the System....1197
25.3.3.2 How to Deploy the Phone Software to System Telephones....1197
25.3.3.3 How to Delete the Phone Software....1198
25.3.3.4 How to Enable or Disable the Automatic Distribution of the Phone Software....1198
25.3.3.5 How to Configure Automatic Re-flashing....1199
25.3.4 Software Status....1200
25.3.4.1 How to Check the Software Status....1200
25.4 Restart, Reload, Shutdown....1200
25.4.1 Restarting OpenScape Business....1201
25.4.1.1 How to Initiate a Restart of OpenScape Business....1202
25.4.2 Reloading OpenScape Business....1202
25.4.2.1 How to Initiate a Reload of OpenScape Business....1203
25.4.3 Shutting Down OpenScape Business X....1203
25.4.3.1 How to Shut Down OpenScape Business X....1204
25.4.4 PIN for the controlled shutdown of OpenScape Business X....1204
25.4.4.1 How to Configure a PIN for the Controlled Shutdown of OpenScape Business X....1204
25.4.5 Restarting (Rebooting) the UC Booster Card (Application Board OCAB)....1205
25.4.5.1 How to Initiate a Restart of the UC Booster Card (OCAB Application Board)....1205
25.4.6 Reloading the UC Booster Card (Application Board OCAB)....1205
25.4.6.1 How to Initiate a Reload of the UC Booster Card (OCAB Application Board)....1206
25.4.7 Restarting the UC Application....1206
25.4.7.1 How to Initiate a Restart of the UC Application....1206
25.5 Inventory Management....1207
25.5.1 System Status....1207
25.5.1.1 How to Check the Station Status....1208
25.5.1.2 How to Check the Status of the Connection Setup....1209
25.5.1.3 How to Check the ITSP Status....1210
25.5.1.4 How to Display IP Addresses....1210
25.5.2 Inventory....1211
25.5.2.1 How to Check the Inventory of OpenScape Business X....1212
25.5.2.2 How to Check the Inventory of OpenScape Business S....1213
25.6 Automatic Actions....1214
25.6.1 Garbage Collection Automatic Action....1214
25.6.1.1 How to Edit the Garbage Collection Action....1214
25.6.1.2 How to Start the Garbage Collection Automatic Action (Activate)....1215
25.6.1.3 How to Stop the Garbage Collection Automatic Action (Deactivate)....1216
25.6.2 DLS Notification Automatic Action....1216
25.6.2.1 How to Edit the DLS Notification Automatic Action....1216
25.6.2.2 How to Start the DLS Notification Automatic Action (Activate)....1217
25.6.2.3 How to Stop the DLS Notification Automatic Action (Deactivate)....1218
25.6.3 Warning Mechanism for SDHC card lifetime....1218

25.6.3.1 How to set a notification in case of errors in SDHC card....1219
25.6.3.2 How to Start the Warning Mechanism for SDHC lifetime Automatic Action.... 1220
25.6.3.3 How to clone and change an SDHC card....1220
25.6.3.4 How to create a SDHC Data Backup File....1221
25.6.3.5 How to replace an SDHC Card....1224
25.7 Power Management....1225
25.7.1 How to Enable or Disable the Power Management.... 1226
25.7.2 How to Change the Ethernet Link Mode the LAN Interfaces.... 1227
25.8 Monitoring and Maintenance of OpenScape Business....1227
25.8.1 Checking the Network Connection of OpenScape Business X.... 1228
25.8.1.1 How to Ping.... 1228
25.8.1.2 How to Test the Trace Route.... 1228
25.8.2 SNMP (Simple Network Management Protocol)....1229
25.8.2.1 How to Display all Communities....1239
25.8.2.2 How to Add a Community.... 1239
25.8.2.3 How to Edit a Community....1239
25.8.2.4 How to Delete a Community.... 1240
25.8.2.5 How to Display Traps.... 1240
25.8.2.6 How to Display Details of a Trap.... 1241
25.8.3 Manual Actions....1241
25.8.3.1 How to Download Diagnostics Data / Diagnosis Logs.... 1244
25.8.4 Traces....1244
25.8.4.1 How to Download a System Trace Log File....1251
25.8.4.2 How to Delete a System Trace Log File.... 1251
25.8.4.3 How to Set Trace Settings to Default Values.... 1252
25.8.4.4 How to Display all Trace Profiles.... 1252
25.8.4.5 How to Start or Stop a Trace Profile....1253
25.8.4.6 How to Display or Edit the Trace Format Configuration....1254
25.8.4.7 How to Display or Edit the Trace Output Interfaces....1254
25.8.4.8 How to Display or Edit Event Viewer and Customer Trace Logs.... 1254
25.8.4.9 How to Download or Open the Event Viewer Log / Customer Trace Log.... 1255
25.8.4.10 How to Clear the Event Viewer Log / Customer Trace Log....1255
25.8.4.11 How to Display M5T Trace Components....1256
25.8.4.12 How to Start or Stop an M5T Trace Component....1256
25.8.4.13 How to Edit M5T Trace Components....1256
25.8.4.14 How to Start or Stop the Secure Trace....1257
25.8.4.15 How to Check the Secure Trace Status....1257
25.8.4.16 How to Change the Secure Trace Password....1257
25.8.4.17 How to Import the Certificate for the Secure Trace from an X.509 File....1258
25.8.4.18 How to Display or Edit the H.323 Stack Trace Configuration....1258
25.8.4.19 How to Edit H.323 Modules....1258
25.8.4.20 How to Download or Open the H.323 Stack Trace Log....1259
25.8.4.21 How to Clear the H.323 Trace Log.... 1259
25.8.4.22 How to Edit the License Component Trace....1260
25.8.4.23 How to Display Details of a Trace Profile....1260
25.8.4.24 How to Stop all Trace Profiles....1260
25.8.4.25 How to Add a Trace Profile....1261
25.8.4.26 How to Display Trace Components....1261
25.8.4.27 How to Display Details of a Trace Component.... 1261
25.8.4.28 How to Start or Stop a Trace Component....1262
25.8.4.29 How to Stop all Trace Components.... 1262
25.8.4.30 How to Set Trace Settings to Default Values.... 1262
25.8.4.31 How to Edit Trace Components.... 1263
25.8.4.32 How to Forward System Log Files automatically.... 1263
25.8.4.33 How to Start the Kernel Crash Data Service....1264
25.8.4.34 How to Stop the Kernel Crash Data Service....1264

25.8.4.35 How to Start Media Server Trace....1265
25.8.4.36 How to Stop Media Server Trace....1265
25.9 TCP Dump....1265
25.9.1 How to Start a TCP Dump....1266
25.9.2 How to Stop a TCP Dump....1266
25.9.3 How to Delete a TCP Dump....1266
25.10 RPCAP daemon....1267
25.10.1 How to Enable the RPCAP Daemon....1267
25.10.2 How to Disable the RPCAP Daemon....1267
25.11 Events....1268
25.11.1 How to Edit Switch Event Logging via a LAN....1270
25.11.2 How to Download the Event Log File....1270
25.11.3 How to Delete an Event Log File....1270
25.11.4 How to Edit E-Mail Settings for Events....1271
25.11.5 How to Display the Event Reaction Table....1271
25.11.6 How to Edit the Reaction Settings for an Event....1272
25.11.7 How to Edit the Reaction Settings for Multiple Events....1272
25.11.8 How to Download or Open Diagnosis Logs....1273
25.11.9 How to Clear Diagnosis Logs....1274
25.11.10 How to Define Destinations for Alarm Signaling....1274
25.12 Configuration Data for Diagnostics....1274
25.12.1 How to Generate Configuration Data for Diagnostics....1275
25.13 Card Manager....1276
25.13.1 How to Use the Card Manager to Write the Communication Software on the M.2 SATA SSD....1277
25.13.2 How to Use the Card Manager to Write the Communication Software on the SDHC Card....1278
25.13.3 How to Use the Card Manager to Write the Communication Software on the OCAB hard disk....1281
25.14 Monitoring and Maintaining the UC Suite....1282
25.14.1 Logging....1283
25.14.1.1 How to Enable or Disable Recording of System Logs....1284
25.14.1.2 How to Enable or Disable the Recording of Client Logs on a System-wide Basis....1284
25.14.1.3 How to Enable or Disable the Recording of Client Logs on a Station-specific Basis....1285
25.14.1.4 How to Configure the Storage Path for Client Log Files....1285
25.14.1.5 How to Enable or Disable Central Storage of Client Logs on the Hard Disk of the Communication System....1286
25.14.1.6 How to Download the Client Logs of all Internal Stations....1286
25.14.2 Notification....1287
25.14.2.1 How to Configure E-mail Notifications of System Errors....1289
25.14.3 Maintenance....1290
25.14.3.1 How to Configure the Time for Maintenance....1291
25.14.3.2 How to Configure Retention Periods for Log Files....1291
25.14.3.3 How to Perform Immediate System Maintenance....1292
25.14.3.4 How to Configure the Retention Period for Contact Center Data....1292
25.15 Monitoring the UC Smart....1292
25.15.1 How to Query the Current Status of UC Smart....1292
25.16 Remote Services....1293
25.16.1 RSP.servicelink....1293
25.16.1.1 How to Install, Configure and Register the RSP.servicelink Plugin....1296
25.16.1.2 How to Enable the RSP.servicelink Plugin....1297
25.16.1.3 How to Disable the RSP.servicelink Plugin....1298
25.16.1.4 How to Reset the RSP Service Plugin....1298
25.16.1.5 How to Configure a PIN for Activating and Deactivating the RSP.servicelink Plugin....1299
25.16.2 Remote Access....1299
25.16.2.1 How to Enable Remote Access via ISDN....1300
25.16.2.2 How to Configure PCs with Microsoft Windows Vista for Remote Access via ISDN....1300
25.16.2.3 How to Configure PCs with Microsoft Windows 7 for Remote Access via ISDN....1302
25.16.2.4 How to Enable Remote Access via Internet Access with a Fixed IP Address....1303

25.16.2.5 How to Enable Remote Access via Internet Access without a Fixed IP Address..... 1303
25.16.2.6 How to Disable Remote Access..... 1304
25.16.3 Online User..... 1305
25.16.3.1 How to Start the Online User..... 1305

26 Migration..... 1307
26.1 Software Upgrade for OpenScape Business X Systems..... 1308
26.1.1 Software Upgrade of OpenScape Business X V2 to OpenScape Business X V3..... 1309
26.1.1.1 SW Upgrade of permanently licensed systems with CLS Connect..... 1309
26.1.1.2 SW Upgrade of permanently licensed systems without CLS Connect..... 1310
26.1.1.3 SW Upgrade of PayGo licensed systems..... 1310
26.2 Software Upgrade of UC Booster Server to OpenScape Business X V3..... 1311
26.2.1 How to Upgrade UC Business Booster Server V2 to V3..... 1311
26.3 Hardware/Software Migration of OpenScape Business X Systems to V3..... 1312
26.3.1 Migration from OpenScape Business X V2 to OpenScape Business X V3..... 1314
26.3.1.1 How to Migrate to V3 Permanently Licensed Systems with CLS Connect..... 1315
26.3.1.2 How to Migrate to V3 Permanently Licensed Systems without CLS Connect..... 1315
26.3.1.3 How to Migrate to V3 PayGo Licensed Systems..... 1316
26.4 Migration of an OpenScape Business X V3 System from V2 Mainboard to V3 Mainboard..... 1317
26.4.1 How to Migrate to V3 Mainboard Permanently Licensed Systems with CLS Connect..... 1319
26.4.2 How to Migrate to V3 Mainboard Permanently Licensed Systems without CLS Connect..... 1319
26.4.3 How to Migrate to V3 Mainboard PayGo Licensed Systems..... 1320
26.5 Software Upgrade of OpenScape Business S..... 1321
26.5.1 Software Upgrade from OpenScape Business S V2 to OpenScape Business S V3..... 1322
26.5.1.1 How to Upgrade to V3 Permanently Licensed Systems with CLS Connect..... 1323
26.5.1.2 How to Upgrade to V3 PayGo Licensed Systems..... 1323
26.5.2 Software Upgrade from OpenScape Business S V2 to OpenScape Business S V3..... 1324
26.6 OpenScape Business V2 Network Migration/Upgrade to V3..... 1325
26.6.1 Scenario 1: Hardware Migration of Master node, Software Upgrade of Slave nodes..... 1326
26.6.1.1 Migration/Upgrade with CLS Connect in the Master Node..... 1326
26.6.1.2 Migration/Upgrade without CLS Connect in the Master Node..... 1327
26.6.2 Scenario 2: Software Upgrade of all Systems in the Network to V3..... 1328
26.6.2.1 Software Upgrade with CLS Connect in the Master Node..... 1328
26.6.2.2 Software Upgrade without CLS Connect in the Master Node..... 1329
26.6.3 Scenario 3a: Software Upgrade of all Nodes..... 1330
26.6.4 Scenario 3b: Software Upgrade in the Master Node, Hardware Migration of the Slave Nodes..... 1330
26.6.4.1 Migration / Upgrade with CLS Connect in the Master Node..... 1330
26.6.4.2 Migration / Upgrade without CLS Connect in the Master Node..... 1331
26.7 Migrating from HiPath 3000 to OpenScape Business V3..... 1332
26.7.1 Migration of HiPath 33xx, 35xx, 3800 to OpenScape Business X3/X5/X8 V3..... 1333
26.7.1.1 How to Load the CDB from HiPath 3000..... 1337
26.7.1.2 How Read out the HG1500 Settings..... 1338
26.7.1.3 How to Convert the HiPath 3000 CDB..... 1338
26.7.1.4 How to Replace the HiPath 3300/3500 Hardware..... 1339
26.7.1.5 How to Replace the HiPath 3350/3550 Hardware..... 1340
26.7.1.6 How to Replace the Hardware for HiPath 3800..... 1341
26.7.1.7 How to Perform the Initial Installation..... 1342
26.7.1.8 How to Load the Converted CDB into the New System..... 1343
26.7.1.9 How to Generate a New License File..... 1343
26.7.1.10 How to Activate a License File Offline..... 1345
26.7.1.11 How to Assign Licenses..... 1345
26.7.1.12 How to Reset the LCR Entries..... 1345
26.7.2 Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V3 with V3 Mainboard..... 1345
26.7.3 Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V3 with UC Booster Server..... 1347

26.7.3.1 How to Convert an OpenScape Office V3 HX Backup Set.... 1349
26.7.4 Migration of a HiPath 3000 network to OpenScape Business network.... 1349
26.7.5 Migration of a HiPath 3000 Internetwork with HiPath 5000 RSM.... 1352
26.7.6 HiPath 3000 Changed/Dropped Features and Interfaces.... 1355
26.8 Migration within OpenScape V3 Business.... 1361
26.9 Migration of HW boards.... 1363
26.9.1 Replacement of SLMO24N with SLMU.... 1363
26.9.2 Replacement of SLM8N with SLMU.... 1363
26.9.3 Replacement of SLCN with SLMUC (SLMU plus CMAe).... 1364
26.10 Migration from OpenScape Business X1 V2 to OpenScape Business X1W V3.... 1364
26.10.1 How to Migrate to X1W V3 Permanently Licensed Systems with CLS Connect.... 1365
26.10.2 How to Migrate to X1W V3 Permanently Licensed Systems without CLS Connect.... 1366

27 Configuration Limits and Capacities.... 1368
27.1 Maximum values for stations.... 1368
27.2 Maximum values for lines.... 1370
27.3 Maximum values for resources.... 1373
27.3.1 Details on the use of DSP channels.... 1374
27.3.2 Details on the use of RTP proxy channels.... 1376
27.4 Maximum values for features.... 1376
27.4.1 Connection to Service Provider.... 1376
27.4.2 Stations.... 1377
27.4.3 UC Smart Expansion Levels.... 1377
27.4.4 Smart Voicemail Expansion Levels.... 1381
27.4.5 UC Suite Expansion Levels.... 1382
27.4.6 Functions at the Telephone.... 1391
27.4.7 Working in a Team (Groups).... 1393
27.4.8 Call Routing.... 1398
27.4.9 Multimedia Contact Center.... 1399
27.4.10 Mobility Expansion Limits.... 1400
27.4.11 Security.... 1401
27.4.12 Networking OpenScape Business.... 1402
27.4.13 Application Connectivity.... 1403
27.4.14 Accounting.... 1405

28 Expert mode.... 1406
28.1 Display Conventions for Parameter Descriptions.... 1406
28.2 **Maintenance**.... 1407
28.2.1 **Configuration**.... 1407
28.2.1.1 **Configuration** > **Music on Hold (MoH)** > **Load to Gateway**.... 1407
28.2.1.2 **Configuration** > **Announcements** > **Load to Gateway**.... 1408
28.2.1.3 **Configuration** > **Port Configuration** 1408
28.2.1.4 **Configuration** > **SmartVM**.... 1409
28.2.1.5 **Configuration** > **SmartVM** > **Mailbox Operations**.... 1409
28.2.1.6 **Configuration** > **SmartVM** > **File Operations**.... 1410
28.2.1.7 **Configuration** > **Branding**.... 1412
28.2.1.8 **Configuration** > **IP Gateway Address**.... 1412
28.2.2 **Software Image**.... 1413
28.2.2.1 **Software Image** > **System Software** > **Update via Internet**.... 1413
28.2.2.2 **Software Image** > **System Software** > **Update via File Upload**.... 1414
28.2.2.3 **Software Image** > **System Software** > **Update via USB Stick**.... 1414
28.2.2.4 **Software Image** > **Phone Images** > **Load**.... 1415
28.2.2.5 **Software Image** > **Phone Images** > **Deploy** 1415
28.2.2.6 **Software Image** > **Phone Images** > **Deploy to device**.... 1416
28.2.2.7 **Software Image** > **Phone Image Logos** > **Load**.... 1416
28.2.2.8 **Software Image** > **Phone Image Logos** > **Deploy**.... 1417

28.2.3 **Cordless**..... 1417
28.2.3.1 **Cordless** > **Base Stations**..... 1417
28.2.4 **Port/Board Status**..... 1419
28.2.4.1 **Port/Board Status** > **Board Status**..... 1419
28.2.4.2 **Port / Board Status** > **Out of Service**..... 1420
28.2.5 **Traces**..... 1421
28.2.5.1 **Traces** > **Trace Format Configuration**..... 1421
28.2.5.2 **Traces** > **Trace Output Interfaces**..... 1422
28.2.5.3 **Traces** > **Trace Log**..... 1423
28.2.5.4 **Traces** > **Digital Loopback**..... 1423
28.2.5.5 **Traces** > **Customer Trace Log**..... 1423
28.2.5.6 **Traces** > **M5T Trace Components**..... 1424
28.2.5.7 **Traces** > **Secure Trace**..... 1424
28.2.5.8 **Traces** > **Secure Trace** > **Secure Trace Certificate**..... 1425
28.2.5.9 **Traces** > **Secure Trace** > **Secure Trace Settings**..... 1425
28.2.5.10 **Traces** > **H.323 Stack Trace**..... 1426
28.2.5.11 **Traces** > **Call Supervision**..... 1427
28.2.5.12 **Traces** > **License Component**..... 1429
28.2.5.13 **Traces** > **Trace Profiles**..... 1429
28.2.5.14 **Traces** > **Trace Components**..... 1430
28.2.5.15 **Traces** > **TCP Dump**..... 1430
28.2.5.16 **Traces** > **rpcap Daemon**..... 1431
28.2.5.17 **Traces** > **Kernel Crash Data**..... 1432
28.2.5.18 **Traces** > **Media Server Trace**..... 1432
28.2.6 **Events**..... 1433
28.2.6.1 **Events** > **Event Configuration**..... 1433
28.2.6.2 **Events** > **Event Log**..... 1433
28.2.6.3 **Events** > **E-mail**..... 1434
28.2.6.4 **Events** > **Reaction Table**..... 1434
28.2.6.5 **Events** > **Diagnosis Logs**..... 1435
28.2.6.6 **Events** > **Alarm Signaling**..... 1435
28.2.7 **Restart / Reload**..... 1436
28.2.7.1 **Restart / Reload** > **Restart / Reload**..... 1436
28.2.8 **SNMP**..... 1437
28.2.8.1 **SNMP** > **Communities**..... 1437
28.2.8.2 **SNMP** > **Communities** > **Read Communities**..... 1438
28.2.8.3 **SNMP** > **Communities** > **Write Communities**..... 1438
28.2.8.4 **SNMP** > **Communities** > **Traps Communities**..... 1438
28.2.8.5 **SNMP** > **Traps**..... 1439
28.2.9 **Admin Log (also called Admin Protocol)**..... 1439
28.2.9.1 **Admin Protocol** > **Configuration**..... 1440
28.2.9.2 **Admin Protocol** > **Admin Log Data**..... 1440
28.2.10 **Actions**..... 1440
28.2.10.1 **Actions** > **Manual Actions** > **Diagnosis Logs**..... 1440
28.2.10.2 **Actions** > **Manual Actions** > **DLI Maintenance**..... 1442
28.2.10.3 **Actions** > **Automatic Actions** > **Garbage Collection**..... 1442
28.2.10.4 **Actions** > **Automatic Actions** > **DLS Notification**..... 1443
28.2.10.5 **Actions > Automatic Actions > SDHC Health Check**..... 1443
28.2.11 **Platform Diagnostics**..... 1444
28.2.12 **Application Diagnostics**..... 1444
28.2.12.1 **Application Diagnostics** > **Developer Settings** > **Trace Console Output**..... 1444
28.2.12.2 **Application Diagnostics** > **Developer Settings** > **Take Over Write Token**..... 1444
28.2.12.3 **Application Diagnostics** > **Mainboard**..... 1444
28.2.12.4 Application Diagnostics> Developer Settings> SIP Provider Profiles..... 1444
28.2.13 **IP Diagnostics**..... 1445
28.2.13.1 **IP Diagnostics** > **Mainboard** > **Address Resolution Protocol**..... 1445

28.2.13.2 **IP Diagnostics > Mainboard > ICMP Request > Ping**....1445
28.2.13.3 **IP Diagnostics > Mainboard > ICMP Request > Traceroute**....1445
28.2.14 **Online User**....1446
28.2.14.1 **Online Users**....1446
28.3 **Telephony**....1446
28.3.1 **Basic Settings**....1446
28.3.1.1 **Basic Settings > System > System Flags**....1446
28.3.1.2 **Basic Settings > System > Time Parameters**....1454
28.3.1.3 **Basic Settings > System > Display**....1460
28.3.1.4 **Basic Settings > System > DISA**....1463
28.3.1.5 **Basic Settings > System > Intercept/Attendant/Hotline**....1463
28.3.1.6 **Basic Settings > System > LDAP**....1466
28.3.1.7 **Basic Settings > System > Texts**....1467
28.3.1.8 **Basic Settings > System > Flexible Menus**....1468
28.3.1.9 **Basic Settings > System > Speed Dials**....1468
28.3.1.10 **Basic Settings > System > Service Codes**....1469
28.3.1.11 **Basic Settings > System > HFA Registration Password**....1470
28.3.1.12 **Basic Settings > Gateway**....1470
28.3.1.13 **Basic Settings > DynDNS > DynDNS Service**....1472
28.3.1.14 **Basic Settings > DynDNS > Update Timer DNS Names**....1473
28.3.1.15 **Basic Settings > Quality of Service**....1474
28.3.1.16 **Basic Settings > Date and Time > Date and Time**....1475
28.3.1.17 **Basic Settings > Date and Time > Timezone Settings**....1475
28.3.1.18 **Basic Settings > Date and Time > SNTP Settings**....1475
28.3.1.19 **Basic Settings > Port Management**....1476
28.3.1.20 **Basic Settings > Call Charges > Call Charges - Output Format**....1477
28.3.1.21 **Basic Settings > Call Charges > Call Charges - Factors**....1479
28.3.1.22 **Basic Settings > Call Charges > Call Charges - Account Codes**....1480
28.3.1.23 **Basic Settings > Announcement Player for Voicemails/Announcements**....1480
28.3.1.24 **Basic Settings > Phone Parameter Deployment**....1480
28.3.1.25 **Basic Settings > Power Management**....1483
28.3.1.26 Basic Installation> Mass Data....1484
28.3.2 **Security**....1485
28.3.2.1 **Security > Application Firewall**....1485
28.3.2.2 **Security > Deployment and Licensing Client (DLSC)**....1486
28.3.2.3 **Security > Deployment and Licensing Client (DLSC) > DLSC Client Certificate**....1487
28.3.2.4 **Security > Deployment and Licensing Client (DLSC) > DLSC CA Certificate**....1488
28.3.2.5 **Security > Signaling and Payload Encryption**....1490
28.3.2.6 **Security > Signaling Encryption/Payload Encryption > SPE Certificate**....1490
28.3.2.7 **Security > Signaling Encryption/Payload Encryption > SPE CA Certificates**....1491
28.3.2.8 **Security > VPN**....1491
28.3.2.9 **Security > VPN > Lightweight CA**....1492
28.3.2.10 **Security > VPN > Certificate Management**....1493
28.3.2.11 **Security > VPN > Certificate Management > Trusted CA Certificates > Active Certificates**....1493
28.3.2.12 **Security > VPN > Certificate Management > Trusted CA Certificates > Configured Certificates**....1494
28.3.2.13 **Security > VPN > Peer Certificates**....1495
28.3.2.14 **Security > VPN > Services > Active Services**....1496
28.3.2.15 **Security > VPN > Services > Configured Services**....1496
28.3.2.16 **Security > VPN > Tunnels > Active Tunnels**....1497
28.3.2.17 **Security > VPN > Tunnels > Configured Tunnels**....1500
28.3.2.18 **Security > VPN > Rules > Active Rules**....1504
28.3.2.19 **Security > VPN > Rules > Configured Rules**....1505
28.3.2.20 **Security > VPN > Public Key Infrastructure (PKI)**....1506
28.3.2.21 **Security > SSL > Certificate Generation**....1507

28.3.2.22 **Security > SSL > Certificate Management**.... 1508
28.3.2.23 **Security > SSL > Certificate Management > Server Certificates**....1508
28.3.2.24 **Security > Web Security**.... 1509
28.3.2.25 **Security > SQL Security**....1510
28.3.3 **Network Interfaces**.... 1510
28.3.3.1 **Network Interfaces > Mainboard > Host Name**....1510
28.3.3.2 **Network Interfaces > Mainboard > LAN 1 (WAN)**.... 1510
28.3.3.3 **Network Interfaces > Mainboard > LAN 2**.... 1515
28.3.3.4 **Network Interfaces > Mainboard > LAN 3 (Admin)**....1516
28.3.3.5 **Network Interfaces > Mainboard > FTP Server**....1517
28.3.3.6 **Network Interfaces > Mainboard > DHCP Mode**.... 1517
28.3.3.7 **Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Global Parameters**.....1518
28.3.3.8 **Network Interfaces > Mainboard > DHCP Mode > DHCP Server > IP Address Pools**.....1519
28.3.3.9 **Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Static IP Addresses**....1521
28.3.3.10 **Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Last active Leases**....1522
28.3.3.11 **Network Interfaces > Mainboard > DHCP Mode > DHCP Server > All Leases**....1522
28.3.3.12 **Network Interfaces > Application Board > Host Name**.... 1523
28.3.3.13 **Network Interfaces > Application Board > LAN 1**.... 1523
28.3.3.14 **Network Interfaces > Application Board > LAN 2**.... 1524
28.3.4 **Routing**....1525
28.3.4.1 **Routing > IP Routing > Mainboard > Static Routes**....1525
28.3.4.2 **Routing > IP Routing > Mainboard > Default Router**.... 1525
28.3.4.3 **Routing > IP Routing > Mainboard > DNS Server**.... 1526
28.3.4.4 **Routing > IP Routing > Application Board > Static Routes** 1526
28.3.4.5 **Routing > IP Routing > Application Board > Default Router**....1527
28.3.4.6 **Routing > NAT**....1527
28.3.4.7 **Routing > PSTN** 1528
28.3.4.8 **Routing > PSTN > PPP Log**....1529
28.3.4.9 **Routing > PSTN > PSTN Partner**....1529
28.3.5 **LCR**.... 1532
28.3.5.1 **LCR > LCR flags**....1533
28.3.5.2 **LCR > Classes Of Service**.... 1533
28.3.5.3 **LCR > Dial Plan**....1533
28.3.5.4 **LCR > Routing Table** 1534
28.3.5.5 **LCR > Dial Rule** 1536
28.3.5.6 **LCR > Multisite**....1538
28.3.6 **Voice Gateway**.... 1538
28.3.6.1 **Voice Gateway > SIP Parameters**....1538
28.3.6.2 Voice Gateway > ITSP Loc-ID Settings....1540
28.3.6.3 **Voice Gateway > Codec Parameters**....1541
28.3.6.4 **Voice Gateway > Destination Codec Parameters**....1543
28.3.6.5 **Voice Gateway > Internet Telephony Service Provider**....1544
28.3.6.6 **Voice Gateway > Networking > Nodes**.... 1555
28.3.6.7 **Voice Gateway > Networking > Routing**....1555
28.3.6.8 **Voice Gateway > SIPQ-Interconnection** 1555
28.3.6.9 **Voice Gateway > Native SIP Server Trunk**.... 1557
28.3.7 **Station**....1562
28.3.7.1 **Station > Station > UP0 Stations**.... 1562
28.3.7.2 **Station > Station > IP Clients**....1565
28.3.7.3 **Station > Station > Analog Stations**.... 1568
28.3.7.4 **Station > Station > ISDN Stations**....1569
28.3.7.5 **Station > Station > DECT Stations > SLC Call number**.... 1570
28.3.7.6 **Station > Station > DECT Stations > DECT Stations**.... 1571
28.3.7.7 **Station > Station > IVM/EVM Ports > EVM**....1572
28.3.7.8 **Station > Station > Virtual Stations**....1573
28.3.7.9 **Station > Station > Station Parameters**....1574

28.3.7.10 **Station > Station > UC Applications**....1585
28.3.7.11 **Station > Station > Profiles/Templates** 1586
28.3.7.12 **Station > Station > DID Extensions**....1588
28.3.7.13 **Station > Station > Mobility Entry**....1588
28.3.7.14 **Station > Station > SfB User**....1589
28.3.7.15 **Station > Station > Overview of Stations**....1590
28.3.7.16 **Station > Key Programming**....1591
28.3.8 **Cordless**....1592
28.3.8.1 **Cordless > System-wide**....1592
28.3.8.2 **Cordless > SLC**....1594
28.3.8.3 **Cordless > Multi-SLC**....1595
28.3.8.4 **Cordless > Base Stations**....1596
28.3.9 **Incoming calls**....1596
28.3.9.1 **Incoming Calls > Groups/Hunt groups**....1596
28.3.9.2 **Incoming Calls > Group Members**....1600
28.3.9.3 **Incoming Calls > Team/top**....1601
28.3.9.4 **Incoming Calls > Call Pickup**....1604
28.3.9.5 **Incoming Calls > UCD**....1605
28.3.9.6 **Incoming Calls > Call Forwarding**....1607
28.3.10 **Trunks/Routing**....1610
28.3.10.1 **Trunks/Routing > Trunks**....1610
28.3.10.2 **Trunks/Routing > Trunk group**....1613
28.3.10.3 **Trunks/Routing > QSIG Features**....1620
28.3.10.4 **Trunks/Routing > Assign MSN**....1621
28.3.10.5 **Trunks/Routing > ISDN Parameters**....1622
28.3.11 **Classes of Service**....1622
28.3.11.1 **Classes of Service > Stations**....1622
28.3.11.2 **Classes of Service > Day: Class of Service Groups**....1623
28.3.11.3 **Classes of Service > Night: Class of Service Groups**....1624
28.3.11.4 **Classes of Service > Allowed Lists**....1624
28.3.11.5 **Classes of Service > Denied Lists**....1625
28.3.11.6 **Classes of Service > Blacklist**....1625
28.3.11.7 **Classes of Service > Night Service**....1626
28.3.11.8 **Classes of Service > CON Group Assignment**....1626
28.3.11.9 **Classes of Service > CON Matrix**....1627
28.3.11.10 **Classes of Service > Autom. night service**....1628
28.3.11.11 **Classes of Service > Special Days**....1629
28.3.12 **Auxiliary Equipment**....1629
28.3.12.1 **Auxiliary Equipment > Music On Hold**....1629
28.3.12.2 **Auxiliary Equipment > PhoneMail**....1630
28.3.12.3 **Auxiliary Equipment > Announcements**....1630
28.3.12.4 **Auxiliary Equipment > Door Opener**....1632
28.3.12.5 **Auxiliary Equipment > SmartVM**....1633
28.3.13 **Payload**....1637
28.3.13.1 **Payload > Devices**....1637
28.3.13.2 **Payload > Media Stream Control (MSC)**....1637
28.3.13.3 **Payload > HW Modules**....1638
28.3.14 **Statistics**....1640
28.3.14.1 **Statistics > Gateway Statics > Mainboard > Device Statistics**....1640
28.3.14.2 **Statistics > Gateway Statistics > Mainboard > MSC Statistics**....1641
28.3.14.3 **Statistics > SNMP Statistics**....1641
28.3.14.4 **Statistics > Telephony Statistics > System Texts**....1642
28.3.14.5 **Statistics > Telephony Statistics > UCD Agents**....1642
28.3.14.6 **Statistics > Telephony Statistics > Trunk Status**....1642
28.3.14.7 **Statistics > Telephony Statistics > Forwarding**....1643
28.3.14.8 **Statistics > Telephony Statistics > Stations**....1643

28.4 **Applications** ... 1645
28.4.1 **Application Selection** ... 1645
28.4.1.1 **Application Selection** ... 1645
28.4.2 **Active Directory Integration Service** ... 1646
28.4.2.1 **Active Directory Integration Service** ... 1646
28.4.3 **UC Smart** ... 1646
28.4.3.1 **UC Smart** > **Basic Settings** ... 1647
28.4.3.2 **UC Smart** > **User Management** ... 1647
28.4.3.3 **UC Smart** > **Status** ... 1648
28.4.4 **OpenScape Business, UC Suite** ... 1649
28.4.4.1 **OpenScape Business, UC Suite** ... 1649
28.4.4.2 **OpenScape Business, UC Suite** > **User Directory** ... 1649
28.4.4.3 **OpenScape Business, UC Suite** > **Departments** ... 1652
28.4.4.4 **OpenScape Business, UC Suite** > **Groups** ... 1652
28.4.4.5 **OpenScape Business UC Suite** > **Templates** ... 1653
28.4.4.6 **OpenScape Business UC Suite** > **External Directory** ... 1654
28.4.4.7 **OpenScape Business UC Suite** > **External Providers Config** ... 1655
28.4.4.8 **OpenScape Business UC Suite** > **Contact Center** ... 1656
28.4.4.9 **OpenScape Business UC Suite** > **Schedules** ... 1664
28.4.4.10 **OpenScape Business UC Suite** > **File Upload** ... 1666
28.4.4.11 **OpenScape Business UC Suite** > **Conferencing** ... 1667
28.4.4.12 **OpenScape Business UC Suite** > **Site List** ... 1667
28.4.4.13 **OpenScape Business UC Suite** > **Server** ... 1668
28.4.4.14 **OpenScape Business, UC Suite** > **Profiles** ... 1674
28.4.4.15 **OpenScape Business, UC Suite** > **Fax Headlines** ... 1676
28.4.5 **Web Services** ... 1676
28.4.5.1 **Web Services** > **Web Collaboration** ... 1676
28.4.6 **Open Directory Service** ... 1677
28.4.6.1 **Open Directory Service** > **Basic Settings** ... 1677
28.4.6.2 **Open Directory Service** > **Data Sources** > **OpenScape Business Users** ... 1677
28.4.6.3 **Open Directory Service** > **Data sources** > **LXV3** ... 1678
28.4.6.4 **Open Directory Service** > **Data sources** > **LXV3** ... 1678
28.4.6.5 **Open Directory Service** > **Maintenance** ... 1678
28.4.7 **Application Launcher** ... 1679
28.4.7.1 **Application Launcher** ... 1679
28.5 **Middleware** ... 1679
28.5.1 Announcement Player ... 1679
28.5.2 Csta Message Dispatcher (CMD) ... 1680
28.5.3 Csta Service Provider (CSP) ... 1680
28.5.4 DSS Server ... 1681
28.5.5 Media Extension Bridge (MEB) ... 1681

29 Appendix ... 1682
29.1 Supported Standards ... 1682
29.2 Euro-ISDN Features ... 1684
29.3 Used Ports ... 1686
29.4 Project Planning of DSP Channels for the OpenScape Business X3/X5/X8 Communication Systems ... 1688

30 Glossary ... 1698
30.1 Glossary ... 1698

Index ... 1713

1 History of changes

Changes mentioned in this chapter are cumulative.

Changes in V3R4 FR3

Impacted chapters	Change description	Issue no.	Date
Trunks/RoutingTrunk group on page 1613	Fix for COLP (ITSP topics)	62	Oct 2025
Wizards - Cloud Services on page 121 CloudLink Service on page 1143 How to configure CloudLink service on page 1144 How to configure CloudLink Daemon web interface on page 1145 How to enable / configure SIP Connector to connect to Workflow Studio on page 1145 (new) CloudLink Pilot Numbers on page 1146 (new) How to configure CloudLink Pilot Numbers on page 1146 (new)	Container Support, Enable SIP Connector and CL Pilot Numbers	62	Sept 2025
Inventory on page 1211	OCCe HW Redesign	62	Sept 2025
Traces License Component on page 1429	Corrected OSBiz-S default and added central license note	64	Jan 2026

Changes in V3R4 FR2

Impacted chapters	Change description	Issue no.	Date
Migration from OpenScape Business X V2 to OpenScape Business X V3 on page 1314	Added note regarding non-default DSP IP address during migration.	61	10 Sept 2025
Auxiliary Equipment Announcements on page 1630	Added link to Configuration > Announcements > Load to Gateway in WAVE file parameter.	60	Sept 2025
Mobility at Home on page 929	Added note regarding limitation with multiple SIP/ HFA devices and NAT.	56	July 2025
Open Directory Service on page 1120	Added note regarding Microsoft Excel - ODS database integration.	56	July 2025
Incoming CallsGroups/Hunt groups on page 1596	Added note regarding dependency with call forward (*1) to another Hunt Group, Call Waiting Group and RNA Group.	56	July 2025
Prerequisites for UC Suite PC Clients on page 516	Updates for Operating systems, Office/Outlook applications, Additional Software (ex. Java / OpenJDK).	56	July 2025

Impacted chapters	Change description	Issue no.	Date
Wizards – Telephones / Subscribers on page 118 Structure of the Administrator Documentation on page 67 Stations on page 406 Mitel SIP DECT stations on page 422 new How to Configure Mitel SIP DECT Stations through Provisioning on page 444 new StationStationStation Parameters on page 1574 How to Configure SIP Stations via Expert Mode on page 446 new	Updates for MITEL SIP-DECT provisioning	55	May-June 2025
Auxiliary Equipment on page 1629 Auxiliary Equipment Announcements on page 1630 Auxiliary Equipment PhoneMail on page 1630 How to Configure Announcements (UC Suite & UC Booster) on page 1176 How to Configure Announcements (UC Smart) on page 1177	Updates for Announcements configuration	55	May-June 2025
Voice GatewayInternet Telephony Service Provider on page 1544	Updates for ITSP profiles	55	May-June 2025

Changes in V3R4 FR1

Impacted chapters	Change description
Team Configuration / Team Group on page 672 Basic MULAP on page 690	Reworked "Ordering of Mulap member devices" paragraph for LAN/WAN with UP.
Installing the Communication Software on page 216	Added note regrading DHCP configuration from yast or WBM.
WBM User Management on page 112	Added note for admin role logging.
SIP Stations on page 418 Group Call on page 653 Hunt Group on page 656	Updates on the list of service codes compatible with SIP devices.

Impacted chapters	Change description
Internet Access on page 160 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP on page 171 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP on page 232 Voice GatewayInternet Telephony Service Provider on page 1544	Updates regarding LAN/WAN and ITSP on WAN.
How to Enable and Configure the Internal DHCP Server on page 142 How to Enable DHCP for Mitel/Unify Devices Only on page 143 How to Enable and Configure the DHCP Server of the Hardware Platform on page 339 Network InterfacesMainboard DHCP ModeDHCP Server Global Parameters on page 1518 Network Interfaces MainboardDHCP Mode DHCP ServerIP Address Pools on page 1519 Network Interfaces MainboardDHCP Mode DHCP ServerStatic IP Addresses on page 1521	Updates for subnet handling DHCP for Mitel/Unify devices and relay option.

Changes in V3R4

Impacted chapters	Change description
Basic MULAP on page 690	Removed SIP phones from being one of the Basic MULAP members.
Details on the use of DSP channels on page 1374	Updates regarding Security and ITSP.
Open Directory Service Data Sources OpenScape Business Users on page 1677	Updates regarding ODS Light.
Voice GatewayNative SIP Server Trunk on page 1557	Direct Media and Payload Encryption for Unify Phone.
Unify Phone on page 1137	Added myAgent to 3rd party call control UC clients.

Impacted chapters	Change description
UC Software Models (Softswitch) on page 102 UC Booster Hardware on page 102 How to Install the Communication Software on page 217 Prerequisites for the Initial Setup on page 211 Initial Setup for OpenScape Business S on page 211 Prerequisites for the Initial Setup on page 265 Initial Setup of OpenScape Business UC Booster on page 263 Initial Setup of OpenScape Business UC Booster on page 263 How to Upgrade UC Business Booster Server V2 to V3 on page 1311	SLES 15 support for OpenScape Business S and UC Booster Server.

Changes in V3R3 FR2 GA Update

Impacted chapters	Change description
Desk Sharing on page 914	Correction for the note concerning the desk sharing feature.
Used Ports on page 257	Consolidation and correction on the used ports for CAR Alive checks.
Open Directory Service Data Sources OpenScape Business Users on page 1677	Correction on the min and max values for max internal and min external lengths and Hide Open calls in Journal button.
Software ImageSystem Software Update via Internet on page 1413	Added missing Clean storage before transferring button.
Unify Phone on page 1137 How to Add Existing Unify Phone Users on page 1140	Added info regarding Unify Phone and 3rd party applications.
OpenScape Business, UC SuiteUser Directory on page 1649 OpenScape Business UC SuiteServer on page 1668	Added two notes regarding different user password lengths and Reset all user passwords.
CloudLink Service on page 1143 How to configure CloudLink service on page 1144 How to open the CloudLink Daemon web interface on page 1144 How to configure CloudLink Daemon web interface on page 1145	Added new chapters for CloudLink service.

Changes in V3R3 FR2

Impacted chapters	Change description
Backup and Restore on page 1179	Added note regarding limitation with Unify Phone Cloud synchronization.
-	Modified UI screen-shots across the document.
Let's Encrypt Service on page 1142	Removed BETA and added new functionality for Let's Encrypt service.
Supported Phones on page 103 Features on page 491 How to Load a Phone Logo into the System on page 1170	Updates for the new supported devices CP205T/ CP405T (TDM).

Changes in V3R3 FR1

Impacted chapters	Change description
Unify Phone on page 1137 How to Configure the Unify Phone Connectivity on page 1137 How to Create New Unify Phone Users on page 1139 How to Add Existing Unify Phone Users on page 1140 How to Edit Unify Phone User Details on page 1141	Updates for Directory and Journal access, numbering scheme screen and trunk access code field.
Wizards - Cloud Services on page 121 Let's Encrypt Service on page 1142	Added 'Cloud Services' wizard and 'Lets encrypt' service.
Open Directory Service on page 1120	Added the 'Open Directory Service and OpenScape Business Mainboards' section.
How to Manage Unify Phone Users on page 1139 How to Create New Unify Phone Users on page 1139 How to Add Existing Unify Phone Users on page 1140 How to Edit Unify Phone User Details on page 1141	Added the 'How to Create New Unify Phone Users' and updated the other chapters accordingly.
How to Customize an Alternative Modern User Interface for myPortal for Desktop OpenScape Business UC Suite Skin Settings Wizards - UC Suite (only with UC Suite) on page 120	Removed files and mentions for 'Skin Settings'.
How to Import a CSV File from the Local File System into the External Directory on page 542 How to Add an External Data Source for the Open Directory Service on page 1127	Updates regarding the 'customer_id' field for import and export of data.

Impacted chapters	Change description
UC SmartBasic SettingsUC Smart Basic Settings on page 1647	Added info regarding CloudService and other missing fields.
How to Configure the Scheduled Night Service on page 732	Added info regarding night mode message on Admin Portal landing page.
Prerequisites for myPortal to go on page 901	Added support via 4G/5G data connections and flat rate data plan recommendation.
Incoming CallsGroups/Hunt groups on page 1596	Added information regarding group type conversions.
How to Remove or Delete Unify Phone Users on page 1141	Edited the delete or remove function for Unify Phone users.
How to Add a Schedule on page 871 How to Edit a Schedule on page 874	Added a note to explain one-to-many linkage of Queues to Schedules.
Working in a Team (Groups) on page 651	Removed chapter "17.1.3 Xpressions Compact" and its entries from the document. Update for reserved hunt groups.
Limiting the Number of Simultaneous Calls via an ITSP on page 781	Added entries for Unify Phone and my Portal for Teams calls.
Classes of ServiceStations on page 1622 How to Change the COS Group for a Voicemail Box Port on page 507	Added notes regarding language setting of class of service groups and EVM port texts.
How to Add the Standard Schedule XYZ for the Sample Contact Center on page 859 How to Add the Standard Schedule Hotline for the Sample Contact Center on page 863 Templates on page 799 Schedules on page 791	Image rebranding and replacement for Contact Center. Reintroduced commented-out image for Schedules chapter.
Schedules on page 840	Removed UCD (incl. Contact Center) and added line regarding Transfer to Queue CVV object.

Changes in V3R3 X1R

Impacted chapters	Change description
Accounting on page 1405 Application Connectivity on page 1403 Call Routing on page 1398 Connection to Service Provider on page 1376 Maximum values for stations on page 1368 Structure and Environmental Conditions on page 102 UC Hardware Models on page 101 DECT stations on page 421 Functions at the Telephone on page 1391 Maximum values for lines on page 1370 Maximum values for resources on page 1373 Mobility Expansion Limits on page 1400 Multimedia Contact Center on page 1399 Networking OpenScape Business on page 1402 Security on page 1401 Smart Voicemail Expansion Levels on page 1381 Stations on page 1377 UC Smart Expansion Levels on page 1377 Working in a Team (Groups) on page 1393	Updates for X1R

Changes in V3R3

Impacted chapters	Change description
Migration on page 1307	Added note regarding deleting Unify phone users.
Updates on page 1188 Licensing on page 282 Networking OpenScape Business on page 995	Added info regarding network - licensing when updating systems.
Reflashing on page 208 Reflashing on page 260	Added two new chapters about reflashing feature.
Licensing Procedure on page 283 Used Ports on page 257 How to Activate CLS Connect on page 298	Removed mentions of obsolete port 7780
Traces on page 1244 Traces on page 1421	Deleted section for RtpProxy Trace, as this trace is no longer available in WBM

Impacted chapters	Change description
Traces Media Server Trace on page 1432 How to Start Media Server Trace on page 1265 How to Stop Media Server Trace on page 1265	New chapters for Media Server
OpenScape Business, UC SuiteUser Directory on page 1649 OpenScape Business UC SuiteServer on page 1668	Updates on date and time format
How to Remove or Delete Unify Phone Users on page 1141	Updates about SDHC card replacement
myPortal for Teams overview on page 1135	myPortal for Teams: call control support
Basic SettingsPhone Parameter Deployment on page 1480	Updates for Canonical dial settings
Migration on page 1307	Added two notes regarding migration good practices and failure points.
How to License Subscribers (Standalone) on page 303 User-oriented Licenses on page 288	Added two notes regarding assigning voicemail licenses.
Software ImageSystem Software Update via File Upload on page 1414 How to Update the System via File Upload on page 1194	Added information regarding the new flag for updating via file upload.
Wrap up on page 847 How to Add a Wrapup Reason for a "Multiple Wrapup" on page 889	Added information regarding multiple wrapup and groups.
How to Activate an Additional LAN Port as a WAN Interface on page 222 How to Select the Country Code and the Language for Trace Logs on page 221 How to Set the Display Logo and Product Name on page 220	Replaced the UI screenshot to display brand with impact in the linked chapters.

Impacted chapters	Change description
How to Configure the Unify Phone Connectivity on page 1137 Wizards - Cloud Services on page 121 How to Configure Internet Access via a Standard ISP PPPoE on page 362 Limiting the Number of Simultaneous Calls via an ITSP on page 781 System Licenses on page 290 Maximum values for stations on page 1368 How to Configure a Predefined ITSP on page 174 How to Configure Internet Access via a Preconfigured ISP on page 165 StationStationStation Parameters on page 1574	Removed chapters and references to the Circuit product.

Changes in V3R2 FR1

Impacted chapters	Change description
How to Configure the Recording of Conferences on page 568 How to Activate or Deactivate the Recording of Calls on page 561	New checkbox in order to enable or disable the recording of conferences
Traces Kernel Crash Data on page 1432 How to Start the Kernel Crash Data Service on page 1264 How to Stop the Kernel Crash Data Service on page 1264	New Kernel Crash Data Service
Possible License Combinations on page 294	Added information about the active licenses needed to use the Contact Center and Company AutoAttendant functions
StationStationStation Parameters on page 1574	Mention that the **Trusted external station call number** field is mandatory
OpenScape Business UC SuiteServer on page 1668	New option to delete after a specified period of time callback messages, live recorded calls, fax calls and emails associated with calls
How to Download a Rule (CCV) as a Backup File on page 876 How to Upload a Downloaded Rule (CCV) in a Backup File Format on page 877	New chapters for downloading and uploading of a rule (CCV)

Impacted chapters	Change description
UC Suite on page 512 Multimedia Contact Center on page 825 Maintenance on page 1167 Expert mode on page 1406	User Interface updates in whole impacted chapters
How to Configure the Sending of E-mails on page 195 OpenScape Business UC SuiteExternal Providers Config on page 1655 OpenScape Business UC Suite Contact Center on page 1656 How to Add Queues for the Sample Contact Center on page 865 How to Add a Queue on page 877 How to Edit a Queue on page 881 How to connect OpenScape Business system to Microsoft Office 365 using Basic Authentication on page 596 How to connect OpenScape Business system to Microsoft Office 365 using Modern Authentication on page 601	Support for OAuth 2.0 authentication
myReports on page 829	myReports administrators can no longer configure the e-mail account to be used for sending reports via e-mail
myPortal for Teams overview on page 1135	myPortal for Teams: support for dial pad and favorites
Prerequisites for myPortal to go on page 901	Updated prerequisites for the myPortal to go iOS client
Subscriber Management on page 817	On myAttendant, the default number of user buttons was increased and can be changed
Users of UC Suite on page 523 OpenScape Business, UC SuiteUser Directory on page 1649	Updated list of supported file formats for uploading a picture

Impacted chapters	Change description
User Access to UC Features (UC Clients) on page 93 Supported Phones on page 103 Deployment Service (DLS and DLI) on page 348 UC Smart Clients on page 468 Prerequisites for myPortal @work on page 471 How to Configure Directories for System Telephones on page 488 Features on page 491 Prerequisites for UC Suite PC Clients on page 516 Team Configuration / Team Group on page 672 OpenScape Business Attendant on page 801 myAttendant on page 815 Prerequisites for myAgent on page 827 How to Load a Phone Logo into the System on page 1170 How to Configure Automatic Re-flashing on page 1199 Software Upgrade for OpenScape Business X Systems on page 1308 How to Upgrade UC Business Booster Server V2 to V3 on page 1311 Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312 Software Upgrade of OpenScape Business S on page 1321 UC Smart Expansion Levels on page 1377 UC Suite Expansion Levels on page 1382 Application Connectivity on page 1403	New supported phones: • OpenScape Desk Phone CP 210 • OpenScape Desk Phone CP 710
Supported Phones on page 103	New supported key modules: • OpenScape Key Module 410 • OpenScape Key Module 710
Basic SettingsSystem LDAP on page 1466	Added note about the display of LDAP sources.
DISA on page 642	Added note regarding calling DISA numbers in OSBiz S and OSBiz X.
OpenScape Business UC SuiteServer on page 1668	Removed DB table entry.
Open Directory Service on page 1120	Modified external data sources and added info regarding the 'Description' field.

Impacted chapters	Change description
How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328	Added text regarding issues with the UC Fax functionality.
Migration from OpenScape Business X1 V2 to OpenScape Business X1W V3 on page 1364	Added chapters regarding Migration from X1 V2 to X1W V3.
Switching from CLS connect on page 298	Introduced Switching from CLS connect chapter.
How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328	Migration OCCLA standalone
Remote Access on page 1299 Overview of functions and codes on page 647 IP Address Scheme on page 132 How to Enable Remote Access via ISDN on page 1300 How to Configure PCs with Microsoft Windows Vista for Remote Access via ISDN on page 1300 How to Configure PCs with Microsoft Windows 7 for Remote Access via ISDN on page 1302	Changed obsolete remote access methods and removed last three chapters.
Migration from OpenScape Business X1 V2 to OpenScape Business X1W V3 on page 1364	Added chapters regarding Migration from X1 V2 to X1W V3.
Voice GatewayNative SIP Server Trunk on page 1557	Added table entries for transport and media security.
OpenScape Business UC SuiteServer on page 1668	Added text regarding the restart of the UC application.
Switching from CLS connect on page 298	Added chapter regarding switching from CLS Connect.
OpenScape Business UC SuiteServer on page 1668	Added text regarding the restart of the UC application.
Voice GatewayNative SIP Server Trunk on page 1557	Added table entries for transport and media security.
Remote Access on page 1299	Removed obsolete remote access methods.
Switching from CLS connect on page 298	Added chapter regarding switching from CLS Connect.

Changes in V3R2

Impacted chapters	Change description
Supported Phones on page 103 Prerequisites for myPortal @work on page 471 Features on page 491 Prerequisites for UC Suite PC Clients on page 516 OpenScape Business Attendant on page 801 myAttendant on page 815 Prerequisites for myAgent on page 827 How to Configure Automatic Re-flashing on page 1199 Significance of Results Obtained from Testing the Radio Area on page 918	New supported phones: • OpenScape Desk Phone CP 110 • OpenScape DECT Phone S6/SL6/R6
myPortal for Teams overview on page 1135	myPortal for Teams: journal support
Expansion Levels Available through Sales on page 97 Maximum values for stations on page 1368 UC Smart Expansion Levels on page 1377 UC Suite Expansion Levels on page 1382 Mobility Expansion Limits on page 1400 Application Connectivity on page 1403	myPortal for Teams: Configuration limits and capacities
myPortal @work on page 469	Camp-on scenarios are supported with myPortal @work
Unify Phone on page 1137 How to Configure the Unify Phone Connectivity on page 1137 How to Manage Unify Phone Users on page 1139 How to Add Existing Unify Phone Users on page 1140 How to Edit Unify Phone User Details on page 1141 How to prepare Alternative number and Call routing for Unify Phone interworking on page 1142 Basic Settings System System Flags on page 1446	New/Updated chapters for Unify Phone connectivity

Impacted chapters	Change description
Licenses on page 285 Possible License Combinations on page 294 User Licenses on page 287 User-oriented Licenses on page 288 System Licenses on page 290 Assigning Licenses (Standalone) on page 301 How to License Subscribers (Standalone) on page 303 Assigning Licenses (Internetwork) on page 311 How to License Subscribers (Internetwork) on page 313	New Unify Phone license
Details on the use of RTP proxy channels on page 1376	Add information about the required RTP proxy channels per Unify Phone call
Presence Status (Presence) on page 532	Added note about presence status visibility.
Users of UC Suite on page 523	Added note about restriction in changing the username.
Licensing on page 282	Renamed OCCLA and OCCL to V3 mainboard and V2 mainboard respectively, in chapters 8.11 to 8.14

Changes in V3R1 FR2

Impacted chapters	Change description
Prerequisites for myPortal to go on page 901	myPortal to go: iOS callkit support
RSP.servicelink on page 1293	Store RSP credentials in backup set
OpenScape Business, UC SuiteGroups on page 1652 OpenScape Business, UC SuiteProfiles on page 1674	UC Suite: Favorites Groups
Trunks/RoutingTrunk group on page 1613 StationStationStation Parameters on page 1574	Trusted SBC
myPortal @work on page 469	myPortal @work: call pick up support
myPortal for Teams overview on page 1135 How to configure myPortal for Teams on page 1136 How to upload myPortal for Teams to Teams store on page 1136	myPortal for Teams

Changes in V3R1 FR1

Impacted chapters	Change description
How to Add an Exception in CCV on page 798	Added new CCV exception type
OpenScape Business UC SuiteServer on page 1668	Added **Disable conversation tracking** parameter
OpenScape Business UC SuiteServer on page 1668	Added **Directory search cache expires in** parameter

Changes in V3R1

Impacted chapters	Change description
• Supported Phones on page 103 • Prerequisites for myPortal @work on page 471 • Deployment Service (DLS and DLI) on page 348 • Features on page 491 • myAttendant on page 815 • Prerequisites for myAgent on page 827 • OpenScape Business Attendant on page 801 • How to Configure Automatic Re-flashing on page 1199 • Software Upgrade for OpenScape Business X Systems on page 1308 • Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312 • Software Upgrade of OpenScape Business S on page 1321 • UC Smart Expansion Levels on page 1377 • UC Suite Expansion Levels on page 1382 • Application Connectivity on page 1403	New supported phone OpenScape Deskphone CP 700 and CP 700X
Supported Phones on page 103	New supported phone OpenScape WLAN Phone WL4/WL4 Plus
• Voice GatewayInternet Telephony Service Provider on page 1544 • Voice GatewayNative SIP Server Trunk on page 1557 • StatisticsTelephony Statistics Trunk Status on page 1642	ITSP improvements
OpenScape Business UC Suite External Directory on page 1654	New button **Remove All**
OpenScape Business UC SuiteServer on page 1668	New flag **Display agent names in myAgent queue binding** for displaying user names along with their extension numbers.
How to display Mass data on page 156	Mass Data is available also in top level menu of Setup Wizards.
Basic Installation> Mass Data on page 1484	Added two new columns **Mobile CallNo** and **Email address**
Classes of Service Autom. night service on page 1628	Added **Copy service** functionality.

Impacted chapters	Change description
• Maximum values for stations on page 1368 • Maximum values for lines on page 1370 • Connection to Service Provider on page 1376 • UC Smart Expansion Levels on page 1377 • Smart Voicemail Expansion Levels on page 1381 • UC Suite Expansion Levels on page 1382 • Working in a Team (Groups) on page 1393 • Mobility Expansion Limits on page 1400 • Application Connectivity on page 1403	Updated maximum values for new boards
• How to Configure the Sending of E-mails on page 195 • How to Edit E-Mail Settings for Events on page 1271 • EventsE-mail on page 1434	Nontify on-site security for emergency calls
• How to Upgrade UC Business Booster Server V2 to V3 on page 1311 • Software Upgrade of OpenScape Business S on page 1321	Security - OpenSSL V1.1.1
How to Forward System Log Files automatically on page 1263	Forwarding Linux Syslog files externally
Basic Installation> Mass Data on page 1484	UC mobile number added in Mass data wizard configuration
How to collect diagnostic traces for error incident on page 207	Automatic diagnostic data collection and transfer

Changes in V3

Impacted chapters	Change description
UC Software Models (Softswitch) on page 102 UC Booster Hardware on page 102 How to Install the Communication Software on page 217 Prerequisites for the Initial Setup on page 211 Initial Setup for OpenScape Business S on page 211 Prerequisites for the Initial Setup on page 265 Initial Setup of OpenScape Business UC Booster on page 263	Update to SLES 12 SP5.
Circuit How to setup Circuit Voicemail number How to setup Alternative number and Call routing for Circuit interworking	Circuit interworking enhancements.

Impacted chapters	Change description
UC Smart User Management on page 1647 Migration within OpenScape V3 Business on page 1361 Possible License Combinations on page 294 User-oriented Licenses on page 288 System Licenses on page 290 Scenario 5: OpenScape Business BLF Connected to an OpenScape Business Single System on page 813 Scenario 6: OpenScape Business BLF Connected to an OpenScape Business Internetwork (BLF and Presence Status via WSI) on page 815 OpenScape Business BLF on page 804 OpenScape Business TAPI 120 on page 1110 Basic Settings for UC Smart on page 465 myPortal @work on page 469	UC Suite licenses for UC Smart clients.
How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328	Block OptiPoint devices on V3 OCC Evolution.
How to Log into the WBM on page 112	Harden external WBM access.
How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328 How to migrate from V2 mainboard to V3 mainboard the master node of a networked system on page 330 How to migrate from V2 mainboard to V3 mainboard the slave node of a networked system on page 331 Migration of HiPath 3000 systems to OSBiz V3 software with V3 mainboard on page 331 Upgrade from V2 to V3 with CLS Connect on page 332 Upgrade from V2 to V3 without CLS Connect on page 332	OCC Evolution.
How to Load a Phone Logo into the System on page 1170	Support CP phone logo load with WBM
Automatic Updates on page 522 myPortal @work on page 469 myPortal @work on page 514	Updates regarding myPortal @work

Changes in V2R7

Impacted chapters	Change description
Wizards – Central Telephony Active Directory Integration Service How to Configure the Active Directory Service Active Directory Integration Service	Added Active Directory Integration Service information
Station > Station > Station Parameters	Deleted PW control deactivation option
Circuit	Added pull/push calls, conference calls and busy in a call information functionality
OpenScape Business UC Suite > Server	Added Disable name editing flag
OpenScape Business, UC Suite > Profiles	Added Hot Keys group in UC Suite Profiles settings
myPortal @work	Added availability on MacOS
UC Software Models (Softswitch) UC Booster Hardware Migration of a HiPath 3000 Standalone System with OpenScape Office V3 HX How to Install the Communication Software Prerequisites for the Initial Setup Initial Setup for OpenScape Business S Prerequisites for the Initial Setup Initial Setup of OpenScape Business UC Booster	Added support of SLES 12 SP3
Voice Gateway > Internet Telephony Service Provider Voice Gateway > Native SIP Server Trunk	Added wiki information (ITSP)

Changes in V2R6FR2

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

- Possible License Combinations
  - Added licenses for myPortal @work VoIP telephony
- myPortal @work
  - Added VoIP information
- Prerequisites for myPortal @work
  - Added VoIP information
- Music on Hold
  - Use of imported MoH in UC Suite

- How to Import Internal Music On Hold
  - Use of imported MoH in UC Suite
- OpenScape Business UC Suite > Server
  - Close conversation after flag added

1.1 History of improvements/fixes

Changes mentioned in this chapter are cumulative.

Changes in V3R4 FR2

Service case ID	Date of change	Description of change	Impacted chapters	Issue no.
PRB000086522	23 Oct 2025	Added section wtih guideines for when increasing subnet range.	Initial Setup for OpenScape Business X on page 128	63
PRB000086522	26 Aug 2025	Added statement about the connection of two ITSPs at the same time on LAN and WAN.	How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP on page 171	59
PRB000081445	18 Aug 2025	Added notes regarding auto generation of media channels.	How to Configure the UC Suite on page 193 How to Configure the UC Suite on page 243	58
PRB000082631	15 Jul 2025	Added information regarding the IP Clients > Device Info, WBM tab, sorting mechanism	StationStationIP Clients on page 1565	57

Changes in V3R4 FR1

Service case ID	Date of change	Description of change	Impacted chapters
PRB000082944	22 Apr 2025	Added a note regrading Unify Phone user data not being part of the export file.	ConfigurationPort Configuration on page 1408

Changes in V3R4

Service case ID	Date of change	Description of change	Impacted chapters
PRB000080604	19 Feb 2025	Modified the sentence about the phone number to be used for outgoing calls when no caller DID number is available.	How to Configure a Predefined ITSP on page 174 How to Configure a Predefined ITSP on page 373
PRB000080170	15 Jan 2025	Correction on the description of the display name / algorithm table entry.	Basic Settings System Display on page 1460

Service case ID	Date of change	Description of change	Impacted chapters
PRB000077322	09 Dec 2024	Correction of both max values for Stations and TDM stations for X1R/W.	Maximum values for stations on page 1368

Changes in V3R3 FR2 GA Update

Service case ID	Date of change	Description of change	Impacted chapters
PRB000079549	15 Sep 2024	Correction on step 5 of email notifications.	How to Configure E-mail Notifications of System Errors on page 1289
PRB000076788	13 Sep 2024	Added note regrading Application Firewall.	Security Application Firewall on page 1485 Application Firewall on page 943 Survivability on page 1087
PRB000075233	18 July 2024	Corrections on the priority of schedules and their exceptions.	How to Add an Exception in CCV on page 798
PRB000077767	28 Aug 2024	Added note regarding Call Forwarding to the Voicemail Box.	Presence Status (Presence) on page 532
PRB000076194	18 July 2024	Correction on the values for used ports of CAR alive checks	Used Ports on page 257

Changes in V3R3 FR2

Service case ID	Date of change	Description of change	Impacted chapters
PRB000076191	13 June 2024	Correction on the values for X1 a/b announcements and MEB channels for X1W/R	Maximum values for lines on page 1370 Maximum values for resources on page 1373
PRB000076108	13 June 2024	Correction on CLS ports and new section at the end of the chapter	Used Ports on page 257

Changes in V3R3 FR1

Service case ID	Date of change	Description of change	Impacted chapters
PRB000072445	1 April 2024	Added the "Maximum local number length" in Canonical Dial Settings	Basic SettingsPhone Parameter Deployment on page 1480
PRB000074047	15 March 2024	Added note to explain how "remove data before import" flag works.	How to Import a CSV File from the Local File System into the External Directory on page 542
PRB000072007	1 April 2024	Added a new chapter "How to Change the Dial Plan to 4 Digits" and related information.	How to Change the Dial Plan to 4 Digits on page 223, System Settings on page 220
PRB000074908	08 April 2024	Added users capacity regarding timed reminders.	Automatic Wake-up System and Timed Reminders on page 647

Service case ID	Date of change	Description of change	Impacted chapters
PRB000073511	14 April 2024	Corrections and fix issue with yearly recurrent exceptions.	How to Add a Schedule on page 871 How to Add an Exception in CCV on page 798

Changes in V3R3

Service case ID	Date of change	Description of change	Impacted chapters
PRB000068453	27 June 2023	Added information regarding Authenticated SMTP and OAuth 2.0.	How to Configure the Sending of E-mails on page 195
PRB000066465	17 Jul 2023	Added information regarding the new port in the firewall for CLS Connect.	Activating Licenses (Standalone) on page 299, Licensing Procedure on page 283, Used Ports on page 257, How to Activate CLS Connect on page 298
PRB000068453	17 Jul 2023	Updated supported image formats.	OpenScape Business, UC SuiteUser Directory on page 1649, Users of UC Suite on page 523
PRB000071258	18 Oct 2023	Added length limits for CSV data.	How to Import a CSV File from the Local File System into the External Directory on page 542
PRB000061414	20 Oct 2023	Added new flag - Use Dedicated Static Route.	Software ImageSystem Software Update via Internet on page 1413
PRB000064083	26 Oct 2023	Added missing values for the Enforce authentication for HFA devices field.	Basic SettingsSystem > HFA Registration Password on page 1470
PRB000071163	24 Nov 2023	Added new chapters and information regarding certificates handling.	Introduction on page 982 (new) How to Import Server Certificates (PEM) on page 986 (new) Certificate Handling for Booster Server on page 989 (new) How to Generate Certificate Signing Requests (CSR) on page 984 How to Generate CA Certificates on page 983 How to Import Server Certificates (PKCS#12) on page 986 Certificate Handling on page 981
PRB000072442	04 Jan 2023	Added note regarding DND behavior in teams.	Team Configuration / Team Group on page 672

Service case ID	Date of change	Description of change	Impacted chapters
PRB000069431	05 Jan 2024	Added info regarding UC Suite, CLI routing, and MS Teams.	Schedules on page 791 Schedules on page 840
PRB000054882	02 Feb 2024	Added info for missing section 'Switched Trunk Authorization'.	Basic SettingsSystem Intercept/ Attendant/Hotline on page 1463
PRB000073109	22 Feb 2024	Added ITSP to SIP trunk channels row in tables.	Maximum values for lines on page 1370
PRB000073818	1 Mar 2024	Correction of the default values for Queue alarm count, Queue alarm time, Missed call timeout, and Abandoned call threshold, parameters.	OpenScape Business UC Suite Contact Center on page 1656

Changes in V3R2 FR1

Service case ID	Date of change	Description of change	Impacted chapters
PRB000066080	11 May 2023	Added note regarding camp on behaviour.	How to Enable or Disable Immediate Call Waiting (Camp On) by the Attendant Console on page 637
PRB000067262	12 May 2023	Corrected MOH delay timer range values.	Basic SettingsSystem Time ParametersTime Parameters, Expert modeBasic Settings System, Expert mode on page 1454
PRB000065660	29 Jun 2023	Added note regarding adding and removing UC contacts.	Directories on page 487, Directories on page 536
PRB000067012	01 Aug 2023	Added note about system speed dialing and toll restriction rules.	System Speed Dialing on page 606
PRB000056655	05 Sep 2023	Added note regarding the display information update after transferring a call.	Transfer on page 620

Changes in V3R2

Service case ID	Date of change	Description of change	Impacted chapters
PRB000052166	20 Jun 2022	Deleted section for Auto DSP Trace, as this trace is no longer available in WBM	Traces on page 1421
PRB000058845	01 Jul 2022	Updated info about the SPE support in networks	Deployment Service (DLS and DLI) on page 348
PRB000058415	22 Aug 2022	Deleted section for Non-Supported Boards and Devices, as this section is moved to the Service Documentation.	Appendix on page 1682
PRB000058021	22 Aug 2022	Updated info about the components to be replaced	Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312

Service case ID	Date of change	Description of change	Impacted chapters
PRB000061111	27 Oct 2022	Added note regarding the VoIP behavior of myPortal@work	UC Smart Clients on page 468
PRB000062363	25 Nov 2022	Added chapter and subchapters regarding migration of HW boards	Migration of HW boards on page 1363
PRB000063445	30 Nov 2022	Added note regarding backup UCD group under basic fallback solution	Fallback solution on page 850
RB000055773, PRB000055775	12 Jan 2023	Added note regarding adding new datasource in ODS.	How to Add an External Data Source for the Open Directory Service on page 1127
PRB000061481	12 Jan 2023	Added note and subchapter regarding deleting Unify Phone users	Unify Phone on page 1137
PRB000063445	12 Jan 2023	Added note under Basic fallback solution	Fallback solution on page 850
PRB000062971	25 Jan 2023	Removed events not present in WBM. Added note and modified table to fit contents.	SNMP (Simple Network Management Protocol) on page 1229
PRB000065939	5 Apr 2023	Changes in the 'Disable myPortal invitation email' flag.	OpenScape Business UC SuiteServer on page 1668
PRB000065939	5 Apr 2023	Changes in the 'Disable myPortal invitation email' flag.	OpenScape Business UC SuiteServer on page 1668
PRB000067211	26 Apr 2023	Added section about migration limitations and workaround.	Migration of an OpenScape Business X V3 System from V2 Mainboard to V3 Mainboard on page 1317

Changes in V3R1

Service case ID	Date of change	Description of change	Impacted chapters
PRB000052438	20 Apr. 2021	Added section for OCCLA and UC Suite/Smart mode	How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328
PRB000051654	14 May 2021	Added new chapters MS Office 365 integration	Microsoft Office 365 Integration Overview on page 595
PRB000051803	19 May 2021	Added note for camp-on scenarios	myPortal @work on page 469
PRB000052202	02 Sept 2021	Added info about Internet calls	Limiting the Number of Simultaneous Calls via an ITSP on page 781

Service case ID	Date of change	Description of change	Impacted chapters
PRB000054381	03 Sept 2021	Remove myPortal Smart entries	• UC Features (Overview) on page 87 • Expansion Levels Available through Sales on page 97 • Languages Supported on page 104 • Key programming on page 427 • UC Smart on page 464 • UC Smart Clients on page 468 • Presence Status (Presence) on page 487 • Networking OpenScape Business X and OpenScape 4000 on page 1065 • HiPath 3000 Changed/Dropped Features and Interfaces on page 1355 • User Access to UC Features (UC Clients) on page 93 • How to License Subscribers (Standalone) on page 303 • myPortal @work on page 469 • myPortal to go on page 899 • Software Upgrade for OpenScape Business X Systems on page 1308
PRB000054046	06 Sept 2021	Added note about devices	Team Configuration / Team Group on page 672Executive/Secretary or Top Group on page 676
PRB000053988	06 Sept 2021	Added note about group name search in myPortal @work	Features on page 491

Service case ID	Date of change	Description of change	Impacted chapters
PRB000054258	10 Sept 2021	Updated chapters for configuring DECT phones	How to Configure the DECT System ID and Other Cordless Parameters (System-wide Data) on page 921 How to Configure Cordless Base Stations on page 922 How to configure DECT Phones for the First Time on page 922 How to Register a DECT Phone (OpenStage/Gigaset Handset) at the Cordless System on page 923 How to Add Additional DECT Phones on page 925 How to Delete DECT Telephones on page 925 How to Configure the Multi-SLC Parameters on page 926 How to Query the Data for Base Stations on page 926 How to Enable the Message Waiting Indication (MWI) for DECT Telephones on page 927 How to Check the Logon Status of DECT Phones on page 927
PRB000051960, PRB000052019	11 Oct 2021	Added note about myPortal@work user account locked in UC Suite mode	myPortal @work user configuration on page 472
PRB000053691	18 Oct 2021	Updated table on how LDAP search is performed	Basic SettingsSystem LDAP on page 1466
PRB000054934	12 Nov. 2021	Added info about the number of conversations that are displayed in the client	myPortal @work on page 469
PRB000054816	03 Feb 2022	Added note about CallMe service	CallMe Service on page 534
PRB000054995/ PRB000055780	18 Feb 2022	Added note for ODBC to ODBC Bridge Server	How to Configure the ODBC to ODBC Bridge Server on page 1125
PRB000055651	28 Feb 2022	Added info about the completion of the DECT phone registration process	How to Register a DECT Phone (OpenStage/Gigaset Handset) at the Cordless System on page 923
PRB000056047	15 Mar 2022	Added note for RSP	RSP.servicelink on page 1293
PRB000055842	30 Mar 2022	Added information about the supported file formats and size limit for uploading a picture	Users of UC Suite on page 523 OpenScape Business, UC SuiteUser Directory on page 1649

Changes in V3

Service case ID	Date of change	Description of change	Impacted chapters
NA16738104	19 Aug. 2020	Added note about filling in both First Name and Last Name fields in external directory	External Directory on page 541
NA16759874	13 Nov. 2020	Added info for full duplex mode support with OCCLA	How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328 Power Management on page 1225 Network InterfacesMainboard LAN 2 on page 1515 Network InterfacesMainboard LAN 3 (Admin) on page 1516 Network InterfacesApplication BoardLAN 1 on page 1523 Network InterfacesApplication BoardLAN 2 on page 1524 Network InterfacesMainboard LAN 1 (WAN) on page 1510
PRB000050351	12 Nov. 2020	Corrected a note about CP0 phones	How to Configure a PIN for the Controlled Shutdown of OpenScape Business X on page 1204
PRB000050248	12 Nov. 2020	Added entries for CAR in the table	Used Ports on page 257
NA16756853/ PRB000049732	10 Dec. 2020	Added note for Booster Server restart in case of configuration changes in e-mail forwarding.	How to Configure the Sending of E-mails on page 590
PRB000050722	15 Dec. 2020	Added info to enable Number conversion for Speed Dial numbers through LDAP.	Rules and Conventions on page 494
PRB000051401	09 Feb 2021	Added note for firewall settings in Device@Home.	Configuration for System Device@Home on page 932
PRB000050983	11 Feb 2021	Added note for number of Circuit users per system.	Maximum values for stations on page 1368
PRB000051647	11 Feb 2021	Added info for Call forwarding after deflect call / single step transfer and Follow call management in case of deflect call / single step transfer flags.	Basic Settings System System Flags on page 1446
PRB000051165	19 Feb 2021	Corrected note with device type.	Executive MULAP on page 693
PRB000050983	15 Feb 2021	Added note for unsupported feature	SIP Stations on page 418

Changes in V2R7

Service case ID	Date of change	Description of change	Impacted chapters
NA16740815	11 Aug. 2020	Added footnote about max number of simultaneous calls in MOH	Maximum values for resources on page 1373

Service case ID	Date of change	Description of change	Impacted chapters
NA16653104	2 Jun. 2020	Documentation Update regarding Used ports	Used Ports on page 257
NA16692823	30 Apr. 2020	Added option to use FQDN also in WAN field of myPortal @work	Prerequisites for myPortal @work on page 471
NA16652178	8 Apr. 2020	Added a note of opening port 8101 in a proxy for proper operation of `CommunicationsServer.exe`.	How to Perform a Silent Uninstallation on page 521 How to Perform a Silent Installation on page 520
NA16582432	6 Apr. 2020	Added information about enabling **Call Supervision**.	Call Supervision on page 622

2 Introduction and Important Notes

This introduction provides you with an overview of the documentation structure. The introduction should assist you in finding information on selected topics faster. Before you begin with the installation and startup of the communication system, make sure that you have carefully read the safety information and warnings as well as the important notes.

INFO: The safety information and requirements inform you about the safety and other requirements to be observed. The important notes contain information on the emergency behavior, the standards and guidelines for the installation, and the radio frequency interference of the communication system. In addition, you will also find details on and the proper disposal and recycling of the communication system here.

2.1 About this Documentation

This documentation describes the administration of OpenScape Business.™.

It includes the hardware models OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 and OpenScape Business X8 as well as the software model OpenScape Business S (softswitch). The UC solution UC Smart is integrated in all OpenScape Business models. The UC solution UC Suite is offered for the hardware models with the optional UC Booster Card or UC Booster Server; in the case of the softswitch, a choice between UC Smart or UC Suite can be made.

NOTICE: The hardware models OpenScape Business X1/X3/X5/X8 (or OpenScape Business X for short) and the Softswitch OpenScape Business S are referred to in this documentation as communication systems.

UC Suite designates the advanced unified communications functions, including the Multimedia Contact Center.

The information in this document contains general descriptions of the technical possibilities, which may not always be available in individual cases. The desired features must be contractually specified for each case.

If a function is not available as described here, this may be due to the following reasons:

- The communication system does not have this feature.
- The required license is not available or activated.

2.1.1 Documentation and Target Groups

The documentation for OpenScape Business is intended for various target groups.

Sales and Project Planning

The following documentation is intended for sales and project planning.

- Feature Description

  This documentation describes all the features. This document is an extract from the Administrator Documentation.

Installation and Service

The following documentation is intended for service technicians.

- OpenScape Business X1/X1W, Installation Guide

  This document describes the installation of the hardware and the initial installation of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Installation Guide

  This document describes the installation of the hardware and the initial installation of OpenScape Business X3/X5/X8.
- OpenScape Business S, Installation Guide

  This documentation describes the initial installation of the OpenScape Business S softswitch.
- OpenScape Business X1/X1W, Service Documentation

  This documentation describes the hardware of OpenScape Business X1.
- OpenScape Business X3/X5/X8, Service Documentation

  This documentation describes the hardware of OpenScape Business X3/X5/X8.
- OpenScape Business X1R, Service and Installation Guide Service Documentation

  This document describes the installation of the hardware, the initial installation and the service of OpenScape Business X1R.

Administration

The following documentation is intended for administrators.

- Administrator Documentation

  This documentation describes the configuration of features that are set up using the OpenScape Business Assistant (WBM). The Administrator documentation is available in the system as online help.
- Configuration for Customer Administrators, Administrator Documentation

  This documentation describes the configuration of features that can be set up using the OpenScape Business Assistant (WBM) with the **Basic** administrator profile.
- Manager E, Administrator Documentation

  This documentation describes the configuration of features that are set up using Manager E.

UC Clients / Telephone User Interfaces (TUI)

The following documentation is intended for UC users.

- myPortal for Desktop, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal for Desktop.
- myPortal for Outlook, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal for Outlook.
- myPortal @work, User Guide

  This documentation describes the installation, configuration and operation of the UC client myPortal @work.
- Fax Printer, User Guide

  This documentation describes the installation, configuration and operation of Fax Printer.
- myPortal to go User Guide

  This documentation describes the configuration and operation of the mobile UC client myPortal to go for smartphones and tablet PCs.
- myAgent, User Guide

  This documentation describes the installation, configuration and operation of the Contact Center client myAgent.
- myReports, User Guide

  This documentation describes the installation, configuration and operation of the Contact Center client myReports.
- myAttendant, User Guide

  This documentation describes the installation, configuration and operation of the attendant console myAttendant.
- OpenScape Business Attendant, User Guide

  This documentation describes the installation, configuration and operation of the attendant console OpenScape Business Attendant.
- UC Smart Telephone User Interface (TUI), Quick Reference Guide

  This documentation describes the voicemail phone menu of the UC solution UC Smart.
- UC Suite Telephone User Interface (TUI), Quick Reference Guide

  This documentation describes the voicemail phone menu of the UC solution UC Suite.

2.1.2 Structure of the Administrator Documentation

This section shows you how the content of the Administrator Documentation is structured. The hardware is described in the Service Documentation.

Section	Contents
Introduction and Important Notes	Overview of the structure of this documentation and important information/ safety information to be observed during installation and operation
System overview	Overview of the communication system for a quick start

Section	Contents
Administration concept	Overview of administration programs and user roles in the WBM
Initial Installation of OpenScape Business X	Integration of OpenScape Business X3/ X5/X8 in the customer LAN and basic configuration using wizards
Initial Installation of OpenScape Business S	Integration of OpenScape Business S in the customer LAN and basic configuration using wizards
Initial Installation of the OpenScape Business UC Booster	Integration of OpenScape UC Business Booster in the customer LAN and basic configuration using wizards
Licensing	Licensing procedures and licenses
Integration into the Internal Data Network (LAN)	LAN/WAN interface, name resolution, data routing, DLI and DLS
Connection to service provider	Internet access, IP telephony, trunk access
Station	Dial plan, IP stations, UP0 stations; DECT stations, Mitel SIP-DECT stations, ISDN and analog stations, virtual stations, users of UC clients, user profiles
UC Smart	Clients and functions of the unified communications solution UC Smart, including Smart Voicemail. Presence status, directories and journal, conferences, team functions, voicemails
UC Suite	CClients and functions of the UC Suite unified communications solution: Presence status and CallMe, directories and journal, conferences and web collaboration, voice and fax messages, instant messaging
Functions at the Telephone	Make calls, call signaling, calling line ID, functions during the call, optimizing communication
Working in a team (groups)	Call pickup group, group call, hunt group, team/top, MULAP, UCD
Call routing	Classes of service, toll restriction, tenant system, LCR, emergency calls
Attendants	AutoAttendants, OpenStage Attendant, PC-based attendants, intercept position
Multimedia Contact Center	Clients and functions of the Contact Center: agents, queues and schedules, VIP service, fallback, reports
Mobility	myPortal to go, Mobility Entry, One Number Service, dual-mode telephony, IP mobility, Cordless/DECT
Security	Firewall, SPE, VPN, certificates

Section	Contents
Networking OpenScape Business	Network plan, networking scenarios, central intercept position, survivability
Auxiliary Equipment	Announcement devices, entrance telephone and door opener, actuators and sensors
Application Connectivity	CSTA, TAPI, Application Launcher
Accounting	Call detail recording, call charges and call duration, cost control
Maintenance	Backup and restore, update, restart, reload, shutdown, factory reset, inventory, actions, remote services
Migration	Upgrading HiPath 3000 to OpenScape Business
Configuration Limits and Capacities	Maximum values for the configuration limits and capacities of the different communication systems
Expert mode	Reference description of the windows/ masks in Expert mode
Appendix	List of supported standards, the Euro-ISDN features and the IP protocols and port numbers used
Glossary	Brief descriptions of commonly used terms

2.1.3 Types of Topics

The types of topics include concepts and tasks:

Type of topic	Description
Concept	Explains the "What" and provides an overview of context and background information for specific features, etc.
Task (operating instructions)	Describes task-oriented application cases (i.e., the "How") step-by-step and assumes familiarity with the associated concepts. Tasks can be identified by the title **How to ...**.

2.1.4 Display Conventions

This documentation uses a variety of methods to present different types of information.

Type of information	Presentation	Example
User Interface Elements	Bold	Click **OK**.
Menu sequence	>	**File** > **Exit**
Special emphasis	Bold	**Do not delete** Name.
Cross-reference text	Italics	You will find more information in the topic*Network*.
Output	Monospace font, e.g., Courier	`Command not found.`
Input	Monospace font, e.g., Courier	`Enter` LOCAL as the file name.
Key combination	Monospace font, e.g., Courier	`<Ctrl>+<Alt>+<Esc>`

2.2 Safety Information and Warnings

Safety information and warnings indicate situations that can result in death, injury, property damage, and/or data loss.

Work on the communication systems and devices should **only** be performed by personnel with proper qualifications.

Within the context of this safety information and these warnings, qualified personnel are people who are authorized to ground and label systems, devices, and trunks and put them into operation in compliance with the applicable safety regulations and standards.

Make sure you have read and noted the following safety information and warnings before installing and starting up the communication system:

Make sure you also read carefully and follow all safety information and warnings printed on the communication system and devices.

Familiarize yourself with emergency numbers.

Types of Safety Information and Warnings

This documentation uses the following levels for the different types of safety information and warning:



DANGER: Indicates an immediately dangerous situation that will cause death or serious injuries.



WARNING: Indicates a universally dangerous situation that can cause death or serious injuries.

CAUTION: Indicates a dangerous situation that can cause injuries.

NOTICE: Indicates situations that can cause property damage and/or data loss.

Additional symbols for specifying the source of danger more exactly

The following symbol is generally not used in this documentation, but may appear on the devices or packaging.

	ESD - electrostatically sensitive devices

Related concepts

Important Notes on page 77

2.2.1 Warnings: Danger

"Danger" warnings indicate immediately dangerous situations that will cause death or serious injury.



DANGER: Risk of electric shock through contact with live wires

- Note: Voltages over 30 VAC (alternating current) or 60 VDC (direct current) are dangerous.
- Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (<1000 VAC), and all work must comply with the national/local requirements for electrical connections.

2.2.2 Warnings: Warning

"Warnings" indicate universal dangerous situations that can cause death or serious injury.



WARNING: Risk of electric shock through contact with live wires

- Use separate ground wires to provide protective grounding for the OpenScape Business X3R, X3W, X5R and X5W communication systems. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Provide protective grounding for each system box of the OpenScape Business X8 communication system with a separate ground wire. Before you start up the system and connect the phones and phone lines, connect the communication system with a permanent earthing conductor.
- Only use systems, tools and equipment which are in perfect condition. Do not use equipment with visible damage.

- Replace any damaged safety equipment (covers, labels and ground wires) immediately.
- Replace the power cable immediately if it appears to be damaged.
- The communication systems and servers should only be operated with outlets that have connected ground contacts.
- During a thunderstorm, do not connect or disconnect lines and do not install or remove boards.
- Disconnect all power supply circuits if you do not require power for certain activities (for example, when changing cables). Disconnect all the communication system's power plugs and make sure that the communication system is not supplied by another power source (uninterrupted power supply unit, for instance).

  Before starting any work, make sure that the communication system is de-energized. Never take it for granted that all circuits have reliably been disconnected from the power supply when a fuse or a main switch has been switched off.
- Expect leakage current from the telecommunications network. Disconnect all telecommunication lines from the communication system before disconnecting the prescribed ground wire from the system.
- As long as the power supply is switched on, always observe the greatest caution when performing measurements on powered components and maintenance work on PC boards and covers.

  Metallic surfaces such as mirrors are conductive. If you touch them, there is a risk of electric shocks or short circuits.

2.2.3 Warnings: Caution

"Caution" warnings indicate a dangerous situation that can result in injury.

CAUTION: Risk of explosion caused by the incorrect replacement of batteries

- Use only the approved battery packs.
- The lithium battery should only be replaced with an identical battery or one recommended by the manufacturer.

CAUTION: Fire hazard

- Only use communication lines with a conductor diameter of 0.4 mm (AWG 26) or more.
- Do not store any documents or similar flammable items in a communication system.

CAUTION: General risk of injury or accidents in the workplace

- After completing test and maintenance work, make sure that all safety equipment is re-installed in the right place and that all covers and the housing are closed.

- Install cables in such a way that they do not pose a risk of an accident (tripping), and cannot be damaged.
- When working on an open communication system or server, make sure that it is never left unattended.
- Use appropriate tools to lift heavy objects or loads.
- Check your tools regularly. Only use intact tools.
- When working on the systems, never wear loose clothing and always tie back long hair.
- Do not wear jewelry, metal watchbands or clothes with metal ornaments or rivets.
- Always wear the necessary eye protection whenever appropriate.
- Always wear a hard hat where there is a risk of injury from falling objects.
- Make sure that the work area is well lit and tidy.

2.2.4 Warnings: Note

"Note" warnings are used to indicate situations that could result in property damage and/or data loss.

The following contains important information on how to avoid property damage and/or data loss:

- Before placing the system into operation, check whether the nominal voltage of the mains power supply corresponds to the nominal voltage of the communication system or server (type plate).
- Follow these ESD measures to protect the electrostatically sensitive devices:
  - Always wear the antistatic wristband in the prescribed manner before performing any work on PC boards and modules.
  - Always place PC boards and modules on a grounded conductive base.
  - Make sure that the components of the communication system (e.g., the boards) are transported and shipped only in the appropriate packaging.
- Use only original accessories. Failure to comply with this safety information may damage the system equipment or violate safety and EMC regulations.
- Sudden changes in temperature can result in condensing humidity. If a communication system or server is transported from a cold environment to warmer areas, for example, this could result in the condensation of humidity. Wait until the communication system or server has adjusted to the ambient temperature and is completely dry before starting it up.
- Connect all cables only to the specified connection points.
- If no emergency backup power supply is available or if no switchover to emergency analog phones is possible in the event of a power failure, then no emergency calls can be made via the communication system following a power failure.
- Before starting wall mounting, check that the wall has sufficient load bearing capacity. Always use suitable installation and mounting materials to mount the communication systems and devices securely.
- Do not allow easily flammable materials to be stored in or near the room where the communication system is installed.

2.2.5 Country-specific Safety Information

Here, you will find information on the specific safety precautions to be observed when installing, starting up and operating the communication systems in certain countries.

2.2.5.1 Safety Information for Australia

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) in Australia:

- The OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) must be installed and serviced only by authorized personnel.
- OpenScape Business wall systems must be installed near the mains socket outlet that supplies power to the respective communication system. The wall socket shall be readily accessible. The integrity of the wall socket must be assured.
- The OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) must be configured to allow emergency calls (for example, 000) to be made at all times.
- If no emergency backup power supply is available or if no switchover to emergency analog phones (trunk failure transfer) is possible in the event of a power failure, then no emergency calls can be made via the communication system following a power failure).
- Music on Hold and paging devices must be connected to the communication system via a Line Isolation Unit approved by the Australian Communications Authority (ACA).

2.2.5.2 Safety Information for Brazil

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) in Brazil:

- The use of the outlet strip with overvoltage protection with part number C39334-Z7052-C33 is absolutely mandatory. The power supply of the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) must be passed through an outlet strip with overvoltage protection.
- The use of shielded Ethernet cables for the LAN/WAN interfaces/ports of the OCCL, OCCM and OCCMR mainboards and the UC Booster Card OCAB (Application Board) is absolutely mandatory.

2.2.5.3 Safety Information for the U.S.

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) in the United States:

- Disruption of the Network and T1

  When communication systems are networked using T1 (1.544 Mbit/s), the telecommunications company (Federal Communications Commission (FCC)) must be notified whenever a communication system is removed from the grid.

  If any of the communication systems of Unify Software and Solutions GmbH & Co. KG described in this documentation disrupts the operation of the public telecommunications network, the telecommunications company is entitled to temporarily block access to the outside line. In general, the telecommunications company will inform you about this in advance. If this is not possible, you will receive notification at the earliest possible time. In this context, you will also be informed that you can lodge a complaint with the telecommunications company.
- Telephone Company Facility Changes

  The telecommunication company is entitled to adapt its own equipment, devices, operating procedures, and processes as necessary; Such modifications may impair the operation of your communication systems. Under normal circumstances, you should be notified in advance so you can maintain uninterrupted telephone service.
- Nonlive Voice Equipment

  Nonlive voice equipment, such as music-on-hold devices and voice recorders must be approved and released by Unify Software and Solutions GmbH & Co. KG and registered in accordance with the rules and regulations of Subpart C of the FCC Rules, Part 68.

  Unreleased devices for voice playback may only be connected through protective circuitry that is approved and released by Unify Software and Solutions GmbH & Co. KG and registered in accordance with the rules and regulations in Subpart C of the FCC Rules, Part 68.
- Ringer Equivalence Number REN

  The Ringer Equivalence Number (REN) is used to determine the number of devices that can be connected to a telephone line so that all the devices ring when that telephone number is called. In most areas, but not all, the sum of the RENs of all devices connected to a line should not exceed five. Contact the local telecommunication company to determine the maximum REN for your calling area.
- New Local Area and CO Access Codes

  Least Cost routing (LCR) must be configured to automatically recognize and take changes in local area codes and CO access codes into account. Otherwise, these codes will not be usable for calls when changes occur.
- Hearing Aid Compatibility

  Emergency phones and public phones (installed in common areas such as lobbies, hospital rooms, elevators, and hotel rooms, for example) must have handsets that are compatible with magnetically coupled hearing aids.

Hearing-impaired individuals who are not in common areas must be provided with hearing-aid compatible handsets, if needed.

All digital phones from Unify Software and Solutions GmbH & Co. KG manufactured after August 16, 1989, are hearing aid compatible and comply with FCC Rules, Part 68, Section 68.316 and 68.317.

- Programmed Dialer features

  When you program emergency numbers or make test calls to emergency numbers with programmed dialer features using products by Unify Software and Solutions GmbH & Co. KG, stay on the line and briefly explain to the dispatcher the reason for the call before hanging up. These activities should be performed during off-peak hours, such early morning or late evening.

- Connecting Off-Premises Station Facilities

  Customers who intend to connect off-premises station (OPS) facilities must inform the telecommunications company of the OPS class for which the equipment is registered and the connection desired.

- Direct Inward Dialing Answer Supervision

  Customers who operate any of the communication systems from Unify Software and Solutions GmbH & Co. KG described in this documentation without providing proper answer supervision are in violation of Part 68 of the FCC rules.

  Every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation returns proper answer supervision to the public switched telephone network (PSTN) when DID calls are:

  – answered by the called station.
  – answered by an attendant.
  – routed to an announcement administered by the customer.

  In addition, every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation also returns proper answer supervision on all DID calls forwarded to the PSTN. Permissible exceptions are when:

  – A call is not answered.
  – A busy tone is received.
  – A congestion tone (reorder tone) is received.

- Equal Access Requirements

  Call aggregators with an increased volume of traffic (such as hotels, hospitals, airports, schools, and so on) must provide end users equal access to the providers of their choice. The current equal access codes (also known as Carrier Access Codes, CACs) are 10xxx and 101xxxx, and 800/888 and 950, where xxx or xxxx represents the provider code.

  To select the provider of choice for a call, the user dials a provider-specific access code before dialing the called party number. Equal access is also obtained by dialing the 800/888 or 950 code of the provider of choice.

  Every communication system of Unify Software and Solutions GmbH & Co. KG described in this documentation is capable of providing user access to interstate providers through the use of equal access codes.

  Modifications by aggregators to alter these capabilities are a violation of the Telephone Operator Consumer Services Improvement Act of 1990 and Part 68 of the FCC Rules.

2.2.5.4 Safety Information for Canada



DANGER: Risk of electric shock through contact with live wires

Only personnel with proper qualifications or qualified electricians should perform work on the low-voltage network (<1000 VAC) and all work must comply with the national/local requirements for electrical connections.

The following safety precautions must always be observed when installing, starting up and operating the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server) in Canada:

- Ringer Equivalence Number REN

  The Ringer Equivalence Number (REN) defines how many devices can be connected to a telephone line at the same time. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.
- Restrictions for connecting devices

  The Innovation, Science and Economic Development Canada (ISED) label identifies certified equipment. This certification means that the equipment meets certain requirements with regard to the protection, operation and security of telecommunication networks. The requirements are documented in the Terminal Equipment Technical Requirements. Innovation, Science and Economic Development Canada (ISED) provides no assurances that certified devices will always operate to the satisfaction of the customer.

  Before installing the equipment and components described in this documentation, it must be ensured that connections to the facilities of the local telecommunications company are permitted. The communication systems and servers must also be installed using an acceptable method of connection. The customer should be aware that compliance with these conditions may not prevent degradation of performance in some situations.

  Repairs to certified equipment should be coordinated by a service technician designated by the manufacturer or supplier. Any repairs or alterations made by the user to any of the equipment or components described in this documentation, or any equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

  To ensure their own safety, users must verify that the electrical ground connections of the power supply, telephone lines and the metallic water pipe system, if present, are interconnected. This precaution may be particularly important in rural areas.

2.3 Important Notes

The important notes inform you about emergency procedures and the proper disposal, recycling, intended use and operating conditions of the communication systems and servers. In addition, they also include details concerning the standards and guidelines for the installation, the radio interference

characteristics of the communication systems, and data protection and data security.

Related concepts

Safety Information and Warnings on page 70

2.3.1 Emergencies

This section provides information on how to proceed in an emergency.

What To Do In An Emergency

First Aid

Calling for Help

Reporting Accidents

- In the event of an accident, remain calm and controlled.
- Always switch off the power supply before you touch an accident victim.
- If you are not able to immediately switch off the power supply, only touch the victim with non-conductive materials (such as a wooden broom handle), and first of all try to isolate the victim from the power supply.
- Be familiar with basic first aid procedures for electrical shock. A fundamental knowledge of the various resuscitation methods if the victim has stopped breathing or if the victim's heart is no longer beating, as well as first aid for treating burns, is absolutely necessary in such emergencies.
- If the victim is not breathing, immediately perform mouth-to-mouth or mouth-to-nose resuscitation.
- If you have appropriate training, immediately perform heart massage if the victim's heart is not beating.

Immediately call an ambulance or an emergency physician. Provide the following information in the following sequence:

- Where did the accident happen?
- What happened?
- How many people were injured?
- What type of injuries?
- Wait for questions.
- Immediately report all accidents, near accidents and potential sources of danger to your manager.
- Report all electrical shocks, no matter how small.

2.3.2 Proper Use

The communication systems and servers may only be used as described in this documentation and only in conjunction with add-on devices and components recommended and approved by Unify Software and Solutions GmbH & Co. KG.

The prerequisites for the proper use of the communication systems and servers include proper transportation, storage, installation, startup, operation and maintenance of the system.

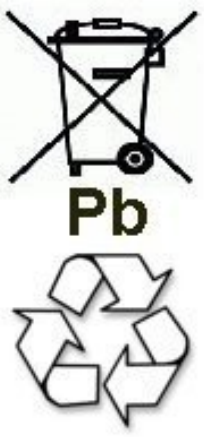
NOTICE: Clean the housing of the communication system and server only with a soft, slightly damp cloth. Do not use any abrasive cleaners or scouring pads.

2.3.3 Correct Disposal and Recycling

Please read the information on the correct disposal and recycling of electrical and electronic equipment and old batteries.



All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities. The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service, the shop where you purchased the product or your sales representative. The statements quoted above are only fully valid for equipment which is installed and sold in the countries of the European Union and is covered by the directive 2012/19/EU. Countries outside the European Union may have other regulations regarding the disposal of electrical and electronic equipment.



Old batteries that bear this logo are recyclable and must be included in the recycling process. Old batteries that are not recycled must be disposed of as hazardous waste in compliance with all regulations.

2.3.4 Installation Standards and Guidelines

This section provides information on the specifications you must comply with when connecting the communication systems and servers to the power supply circuit and when using shielded cabling for LAN and WAN connectors.

2.3.4.1 Connecting OpenScape Office X to the Power Supply Circuit

The OpenScape Business X communication systems have been approved for connection to TN-S power supply systems. They can also be connected to a TN-C-S power supply system in which the PEN conductor is divided into a ground wire and a neutral wire. TN-S and TN-C-S systems are defined in the IEC 60364-1 and IEC60364-5-51 standard.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect the communication systems must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations.

2.3.4.2 Connecting OpenScape Business S and OpenScape Business UC Booster Server to the Power Supply Circuit

For information regarding the connection of OpenScape Business S and OpenScape Business UC Booster Server (Application Server) to the power supply circuit, please refer to the manufacturer's documentation for the server PC and the other components.

Only qualified electricians should perform any work that may be required on the low-voltage network. These installation activities to connect OpenScape Business S and the OpenScape Business UC Booster Server must be performed in compliance with IEC 60364-1 and IEC 60364-4-41 or any corresponding legal norms or national regulations (for example in the U.S. and in Canada).

2.3.4.3 Shielded Cabling for LAN and WAN Connections of OpenScape Business X

Compliance with CE requirements on electromagnetic compatibility in the OpenScape Business X communication systems and their LAN and WAN connections is subject to the following conditions:

- The communication systems should only be operated using shielded connection cables. This means that a shielded Category 5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN and WAN sockets of the communication systems and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building’s potential equalization terminal).
- A shielded Category 5 (CAT.5) cable should also be used for shorter connections with external active components (LAN switch or similar). However, the active component must feature a shielded LAN connection with a grounded shield connection (connection to the building’s potential equalization terminal).

- The shield properties of the cable components should at least satisfy the requirements of the European standard EN 50173-1*) "Information technology - Generic cabling systems" (and all references specified).***)
- Building installations that are fitted with shielded symmetrical copper cables throughout in accordance with the Class-D requirements**) of EN 50173-1 satisfy the above condition.***)

2.3.4.4 Fire Safety Requirements

Fire safety requirements are defined on a country-specific basis in the building regulations. Please follow the valid regulations for your country.

To ensure the legal fire protection and EMC requirements, operate the OpenScape Business X communication systems only when closed. The system may only be opened temporarily for installation and maintenance purposes.

OpenScape Business system cables comply with the requirements of international norm IEC 60332-1 regarding flammability. The following norms contain similar requirements regarding cables:

IEC 60332-1 Note: IEC 60332-1 is equivalent to test method UL VW-1	EN 60332-1-1 and EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) and DIN EN 60332-2-1 (VDE 0482-332-2-1)

The division responsible for project planning and service must check whether the IEC 60332-1 norm complies sufficiently with the relevant building regulation and any other applicable regulations.

2.3.4.5 Lightning Protection Requirements

The protection of communication systems against high-energy surges requires a low-impedance ground connection in accordance with the specifications in the *OpenScape Business Installation Guide*.

NOTICE: Once a communication system has been grounded, check the low-impedance ground connection of the system using the ground conductor of the mains power supply circuit and the low-impedance connection (of the additional

*) The European standard EN 50173-1 is derived from the international standard ISO/IEC 11801.

**) Class-D is reached, for instance, if Category-5 (CAT.5) components (cables, wall outlets, connection cables, etc.) are installed.

***) UTP cables (U.S. standard EIA/TIA 568 A/B) are the most widely used cables on the North American market; this has the following implications for the LAN and WAN connections in communication systems: The systems may only be operated with shielded connection cables. This means that a shielded Category 5 (CAT.5) cable with a length of at least 3 m should be used between the shielded LAN and WAN sockets of the communication systems and the building installation port or the external active component port. The cable shield must be grounded at the building installation end or the external active component end (connection to the building's potential equalization terminal).

permanently-connected protective ground conductor) to the building's potential equalization bus.

NOTICE:

Fire hazard due to surge voltage

Telecom lines which are over 500m in length or which must leave the building must be conducted through an additional external lightning protection.

Lightning protection of this kind is known as additional primary protection. The additional primary protection is guaranteed by the professional installation of ÜSAGs (surge arresters, gas filled) in the main distribution frame, the patch panel or at the entry point of the pipe in the building. A gas-filled surge arrester with 230 V nominal voltage is switched to ground from each wire that is to be protected.

Without this additional primary protection, lightning could irreparably damage the boards. This can cause the entire communication system to fail or result in components overheating (Fire hazard).

2.3.4.6 Markings for OpenScape Business X



The compliance of the equipment according to EU directives is confirmed by the CE mark. This Declaration of Conformity and, where applicable, other existing declarations of conformity as well as further information on regulations that restrict the usage of substances or affect the declaration of substances used in products can be found in the Unify Expert WIKI at http://wiki.unify.com under the section “Declarations of Conformity”.

2.3.5 Notes on Electromagnetic and Radio Frequency Interference of OpenScape Business X

The OpenScape Business X communication systems are Class B devices in accordance with EN 55032.

2.3.6 Data Protection and Data Security

Please note the details below with respect to protecting data and ensuring privacy.

The communication systems and servers described in this documentation process and use personal data for purposes such as call detail recording, displays, and customer data acquisition.

In Germany, the processing and use of such data is subject to various regulations, including those of the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). For other countries, please follow the appropriate national laws.

The aim of data protection is to protect the rights of individuals from being adversely affected by use of their personal data.

In addition, the aim of data protection is to prevent the misuse of data when it is processed and to ensure that one's own interests and the interests of other parties which need to be protected are not affected.

INFO: The customer is responsible for ensuring that the communication systems and servers are installed, operated and maintained in accordance with all applicable labor laws and regulations and all laws and regulations relating to data protection, privacy and safe labor environment.

Employees of Unify Software and Solutions GmbH & Co. KG are bound to safeguard trade secrets and personal data under the terms of the company's work rules.

In order to ensure that the statutory requirements are consistently met during service – whether on-site or remote – you should always observe the following rules. You will not only protect the interests of your and our customers, you will also avoid personal consequences.

A conscientious and responsible approach helps protect data and ensure privacy:

- Ensure that only authorized persons have access to customer data.
- Take full advantage of password assignment options; never give passwords to an unauthorized person orally or in writing.
- Ensure that no unauthorized person is able to process (store, modify, transmit, disable, delete) or use customer data in any way.
- Prevent unauthorized persons from gaining access to storage media such as backup CDs and DVDs or log printouts. This applies to service calls as well as to storage and transport.
- Ensure that storage media which are no longer required are completely destroyed. Ensure that no sensitive documents are left unprotected.
- Work closely with your customer contact; this promotes trust and reduces your workload.

2.3.7 Technical Regulations and Conformity of OpenScape Business X

Details on how the OpenScape Business X communication systems meet conformity requirements can be found here.

2.3.7.1 CE Conformity

The CE certification is based on: 2014/35/EU - Low Voltage Directive (LVD); (Official Journal of the EU L96, 29.03.2014, p. 357-374) 2014/30/EU - Electromagnetic Compatibility Directive (EMC); (Official Journal of the EU L96, 29.03.2014, p. 79-106) 2011/65/EU - Restriction of the use of certain Hazardous Substances Directive (RoHS); (Official Journal of the EU L174, 01.07.2011, p. 88–110)

	Standards reference
Safety	EN 62368-1
Electromagnetic Compatibility EMC	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

2.3.7.2 Conformity with US and Canadian Standards

	Standards reference
Safety USA and Canada	CSA/UL 62368-1
EMC Emission Canada	ICES-003 Issue 6 Class B
EMC Emission USA	FCC 47 CFR Part 15 Subpart B Class B

FCC Registration Number and Power Consumption

A label on the rear of the housing of the communication systems identifies the FCC registration number, the ringer equivalence number (REN), and other information. Upon request, this information may be disclosed to the telecommunication company.

2.3.7.3 Conformity with International Standards

	Standards reference
Safety	IEC 60950-1 and IEC 62368-1
EMC Emission	CISPR 32

2.3.8 Operating Conditions

Note the environmental and mechanical conditions for operating the OpenScape Business X and OpenScape Business S communication systems and the OpenScape Business UC Booster Server (Application Server).

2.3.8.1 Operating Conditions for OpenScape Business X

The environmental and mechanical conditions for operating the OpenScape Business X communication systems are specified.

Environmental Operating Conditions

Operating limits:

- Room temperature: + 5 to + 40 °C (41 to 104 °F)
- Absolute humidity: 1 to 25 g H_2O/m^3
- Relative humidity: 5 to 80%

Ventilation of the communication systems is by convection only. Forced ventilation is required for OpenScape Business X5W when using more than 32 a/b interfaces.

NOTICE: Damage caused by local temperature increases

Avoid exposing the communication systems to direct sunlight and other sources of heat.

NOTICE: Damage caused by condensation due to humidity

Avoid any condensation of humidity on or in the communication systems before or during operation under all circumstances.

A communication system must be completely dry before you put it into service.

Mechanical Operating Conditions

The communication systems are intended for stationary use.

2.3.8.2 Operating Conditions for OpenScape Business S and OpenScape Business UC Booster Server

For details on the environmental and mechanical conditions for operating OpenScape Business S and OpenScape Business UC Booster Server (Application Server), please also refer to the manufacturer documentation of the server PCs and the other components.

3 System Overview

OpenScape Business offers small and medium-sized businesses the answer to their individual and diverse communication needs in a unified, flexible and scalable solution. The OpenScape Business solution architecture can be deployed independently of the existing telephony infrastructure, regardless of whether traditional telephony, IP or DECT is involved. From powerful telephony to a comprehensive Unified Communications (UC) solution, OpenScape Business always provides the right solution.

Flexible, scalable and powerful

OpenScape Business combines the best of HiPath 3000 and OpenScape Office in a new solution platform.

3.1 Highlights

OpenScape Business is the all-in-one solution for small and medium-sized enterprises and offers the following highlights.

Highlights

- Integrated voice services, presence management (presence status), drag and drop conferencing, visual voicemail (voicemail box), AutoAttendant, Multimedia Contact Center, IM (Instant Messaging), Mobility, directory access with database connection, fax, integration into business processes, and much more
- UC clients individually customized for the workplace and way of working
- Interface integration of OpenScape Web Collaboration
- The perfect solution for customers with one location or network-wide solution with multiple locations
- OpenScape Business offers a unified business solution architecture.
- Depending on the existing infrastructure, different OpenScape Business models are available for various configuration sizes. Alternatively, it is possible to run the OpenScape Business software on a standard server (Softswitch) - also in fully virtualized environments, of course.
- The UC solution UC Smart is already provided on the mainboard. The additive UC solution UC Suite supports a larger number of UC users and offers an expanded scope of UC features. A UC Booster Card or a UC Booster Server is required for this.
- All communication interfaces are already available for diverse and heterogeneous requirements: IP, digital, analog and DECT, as well as all common trunk interfaces for voice communication

3.2 Unified Communications

Unified Communications (UC) is a technology that improves communication in enterprises by integrating various communication media in a unified application environment. Unified Communications simplify business processes in enterprises through an integrated presence management (e.g., calls are routed automatically to the mobile phone when the user is out of the office). Several other features such as dial-in conferencing, personal voicemail (voicemail box), personal fax box, Instant Messaging (IM), use of the mobile phone as

an extension of the communication system, Contact Center, video and web collaboration, etc., are also combined in this unified solution.

With the flexible unified communications approach of OpenScape Business, a number of different UC solutions are offered, depending on the requirements at the workplace and the existing infrastructure. For the UC solution, you can choose between UC Smart and UC Suite (both cannot be used simultaneously).

The UC Smart solution already integrated in OpenScape Business can be migrated to the advanced UC Suite solution at any time via an upgrade license. Depending on the number of UC subscribers, OpenScape Business must then only be expanded with the internal board "UC Booster Card" or the external Linux server "UC Booster Server". As a pure softswitch, OpenScape Business S is available as a server solution with the optional UC Smart or UC Suite.

3.2.1 UC Features (Overview)

Depending on the selected UC solution (UC Smart or UC Suite) different UC functions are available to you.

The following tables are intended to help you choose the best UC solution for your requirements. Detailed functional constraints can be found in the relevant sections (UC Smart, UC Suite, Attendants) of the Feature Description and Administrator Documentation.

UC feature	**UC Smart**	**UC Suite**			**Notes**
	myPortal to go	**myPortal for Desktop/ Outlook**	**myPortal @work**	**myPortal to go**	
Presence Status					
Presence status (presence management)	x	x	x	x	
Change presence status via the Client	x	x	x	x	
Change presence status via the TUI	-	x	-	-	
Status-based call forwarding	x	x	x	Via destinations defined in myPortal	With UC Smart, any number can be selected as the destination. With UC Suite, only a number from the preselection can be selected.
Status display in favorites	x	x	x	x	
Status display in directories	x	x	x	x	

UC feature	UC Smart	UC Suite			Notes
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Status display in the Journal	-	x	-	-	
Enable CallMe service	-	x	x	x	
Calendar integration (Outlook)	-	x	-	-	
Calendar integration (iCal) (only with myPortal for Desktop)	-	x	-	-	
Favorites					
Display call status	x	x	x	x	
Create groups	x	x	-	-	
Compact display of favorites	-	x	-	-	
Directories					
Personal directory	x	x	x	x	
Internal directory	x	x	x	x	
External directory	-	x	x	x	
Search in directories	x	x	x	x	
Access to speed-dial destinations defined in the system (SSD)	x	-	x	x	
Import / Manage personal contacts (CSV / XML)	-	x	-	-	
Access to Outlook Contacts	-	x	-	-	
Import of personal contacts (Mac OS) (myPortal for Desktop)	-	x	-	-	
Integration of external directory server via LDAP	-	x	-	-	
Journal					
All calls	x	x	-	x	
Open calls	-	x	-	-	
Missed calls	x	x	-	x	
Answered calls	x	x	-	x	
Scheduled calls	-	x	-	-	
Voicemail	x	x	-	x	
Fax journal	-	x	-	-	
Conversations					
Chat	-	-	-	-	
Journal	-	-	x	-	

UC feature	UC Smart	UC Suite			Notes
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Voicemail	-	-	x	-	
Calls					
Manual dialing	x	x	x	x	
Desktop dialer (click to call)	-	x	-	-	
Forwarding	x	x	x	x	
Place call on hold	x	x	x	x	
Record calls (voice recording)	-	x	-	-	
Send email	x	x	x	x	
Send SMS	x	-	-	x	
Start chat	-	x	-	-	
Popups	-	x	-	-	
Conferences					
AdHoc conference	x	x	x	x	
Scheduled conferences	-	x	-	-	
Permanent and open conferences (drag & drop conference)	-	x	-	-	
Web collaboration integration	-	x			
Voice and fax messages					
Voicemail box (visual voicemail)	x	x	x	x	Voicemail functionality for subscribers (IP, TDM)
Playback through phone	x	x	x	x	
Playback through PC sound card	-	x	-	-	
How to Send a Voice Message as an Email	x	x	-	-	
Fax	-	x	-	-	
Instant messaging					
Instant messaging (chat)	-	x	-	-	

1 myPortal to go also allows access to the local smartphone contacts.

Contact Center

UC feature	UC Smart	UC Suite		Notes
		myAgent	myReports	
Agents, queues and schedules	-	x	-	
Fax and email	-	x	-	
Predefined reports/ report templates	-	x	x	
Scheduled creation of reports	-	-	x	

Optionally, the connection of OpenScape Contact Center is possible.

Attendants (Attendant Consoles)

UC feature	UC Smart	UC Suite	Notes
	Business Attendant	myAttendant	
Display of waiting calls with call type, name and phone	x	x	
Display connection status	x	x	
Fast switching of calls	x	x	
Speed-dialing via BLFs and user buttons. Individual configuration of the busy lamp fields and user buttons with call number or name	x	x	
View presence status of other subscribers	x	x	With OpenStage Business Attendant, presence requires the UC Booster Card/Server or Business S
Change presence status of other subscribers	x	x	
Personal directory	-	x	
Internal directory	x	x	
External directory	x	x	
Outlook Contacts	x	x	
LDAP access	x	x	
Journal	-	x	
AdHoc conference	x	x	
Scheduled, permanent and open conferences (drag & drop conference)	-	x	

UC feature	UC Smart	UC Suite	Notes
	Business Attendant	myAttendant	
Message Center	-	x	All voicemails, faxes, instant messages as well as SMS messages and emails are recorded and managed via the Message Center
Access to voicemail and fax messages of other subscribers	-	x	Must be released by each respective subscriber
Instant messaging (chat)	-	x	
Night service	x	x	

The recommended Attendant client for UC Suite is myAttendant. However, OpenScape Business Attendant can also be used with UC Suite.

Voicemail & Company AutoAttendant

UC feature	UC Smart	UC Suite	Note
Basic functionality of UC Smart Voicemail & Company AutoAttendant	x	-	
Basic functionality of UC Suite Voicemail & Company AutoAttendant	-	x	Requires UC Booster Card/ Server or Business S
UC Features			
Graphical operation of voicemail for subscribers (web interface or client interface)	x	x	
Voicemail prompts for presence function	x	x	Different announcements, depending on the set UC presence
Personal rules for greetings per mailbox	-	x	The subscriber defines detailed rules for the selection of his or her personal greetings
Voicemail to Email	x	x	Voicemail is attached to email as a wave file
AutoAttendant functions			
Attendant mailboxes (Basic AutoAttendants)	100	20	
Company AutoAttendant	x	x	Central attendant console and centralized voicemail with alternative greetings for each extension

UC feature	UC Smart	UC Suite	Note
Announcement prior to answer / Parallel signaling	x	x	Announcement to the caller while the subscriber is being called For UC Suite, this is only possible in conjunction with the Contact Center
Dial-in destinations for 4 day sections / Calendar for AutoAttendant	x	x	Variable automated Attendant for different times of the day Calendar function possibly with UC Smart via the automatic night service
Central calendar for mailbox	x	x	Announcements and call handling for company-wide events such as holidays, company holidays, etc.
Custom profiles for mailbox and personal AutoAttendant	-	x	Presence-based call handling that can be individually set per subscriber
Schedules	Day and Night service	Schedule with rules (Call Control Vector, CCV)	
Templates	1 AutoAttendant configured by default	5 customizable templates	
Graphical rule editor (CCV editor)	-	x	
Concatenation of mailboxes / Multi-step AutoAttendant	x	-	The call is forwarded from one concatenated mailbox to the next, and each time the respective announcement is played
Dial by Name	-	x	
Dial by Extension	x	x	
Voicemail features			
Personalized greetings per mailbox	4	10	Save and set various announcements
Forwarding of voice messages	-	x	Forward message to another subscriber/ mailboxes
Callback from the voicemail box	x	x	Callback to the caller of the message can be activated

UC feature	UC Smart	UC Suite	Note
Notification call	-	x	When a message arrives, a call is made to an external destination, e.g., a mobile phone
Representative function	-	x	Forward caller to representative with personal announcement
Caller-based voicemail / CLI routing	-	x	Call number-based handling, e.g., a greeting in the language of the caller
Central group mailbox	x	x	With announcements for departments / groups
Live Recording	-	x	Recording of conversations with security functions In OpenScape Business S in which live recording from UC is used, G.729A is not considered.
Save messages	-	x	Subscribers can save individual voicemail messages for themselves
Automatic deletion of messages	x	x	After a retention period, messages are deleted to free storage space
Switch voicemail box language on subscriber-specific basis	-	x	Selection of automatic announcements in individual language

Related concepts

UC Smart on page 464

3.2.2 User Access to UC Features (UC Clients)

Access to the UC features occurs via UC clients. The presence status (UC Suite) and voicemail (UC Smart and UC Suite) can also be accessed through the telephone user interface (TUI).

UC clients are offered for the major operating systems. Please also note the requirements of the clients in the respective release notes.

Communication Clients (Desktop and Groupware Clients)

Client	Recommended for		Description
	UC Smart	UC Suite	
myPortal @work	x	x	UC Desktop Client for Microsoft Windows and Mac OS X
myPortal for Desktop	-	x	Advanced UC Desktop Client for Microsoft Windows and Apple Mac
myPortal for Outlook	-	x	UC Groupware Client for Microsoft Outlook Integration
OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (integrated Client to phone software)	x	x	Presence control and phonebook access for UC Suite and UC Smart

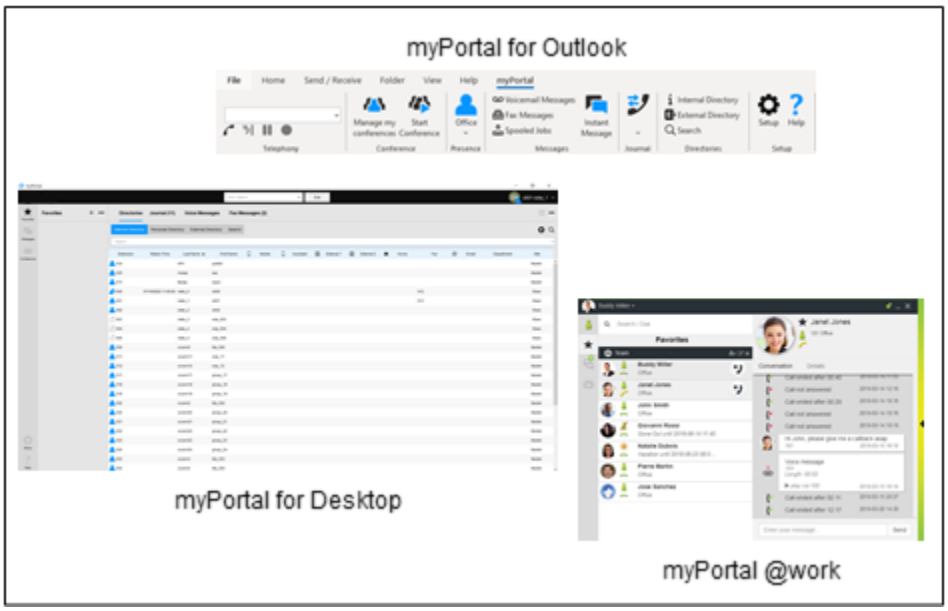


Figure 1: myPortal for Desktop, myPortal for Outlook and myPortal @work

Mobility Clients

Client	Recommended for		Description
	UC Smart	UC Suite	
myPortal to go	x	x	Mobile app for smartphones and tablet PCs myPortal to go is available for UC Smart and UC Suite with slightly different features



Figure 2: myPortal to go

Contact Center Clients

Client	Recommended for		Description
	UC Smart	UC Suite	
myAgent	-	x	Contact Center Client
myReports	-	x	Reports/Reporting interface for Contact Center myReports can be also be used for system statistics independently of the Contact Center

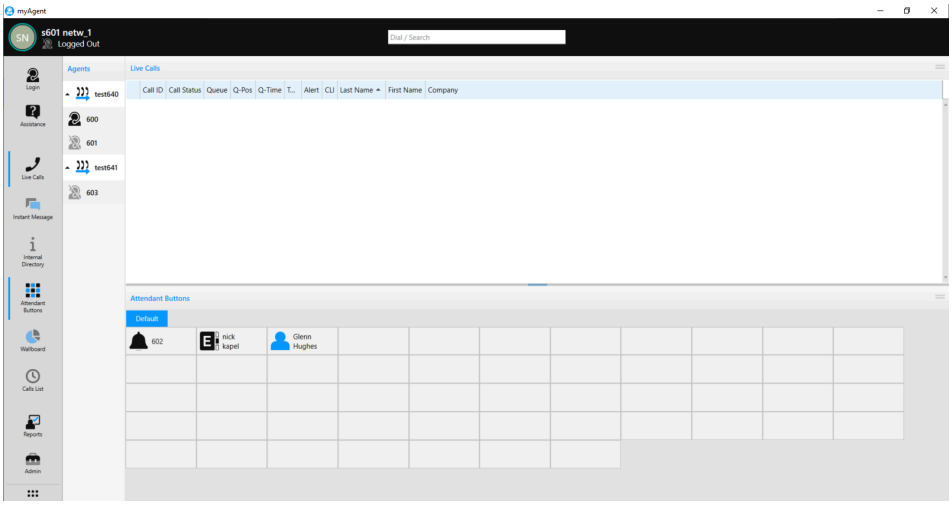


Figure 3: myAgent

Attendants/Attendant Consoles

Client	Recommended for		Description
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	UC Attendant Console including presence
myAttendant	-	x	Advanced UC Attendant Console for UC Suite

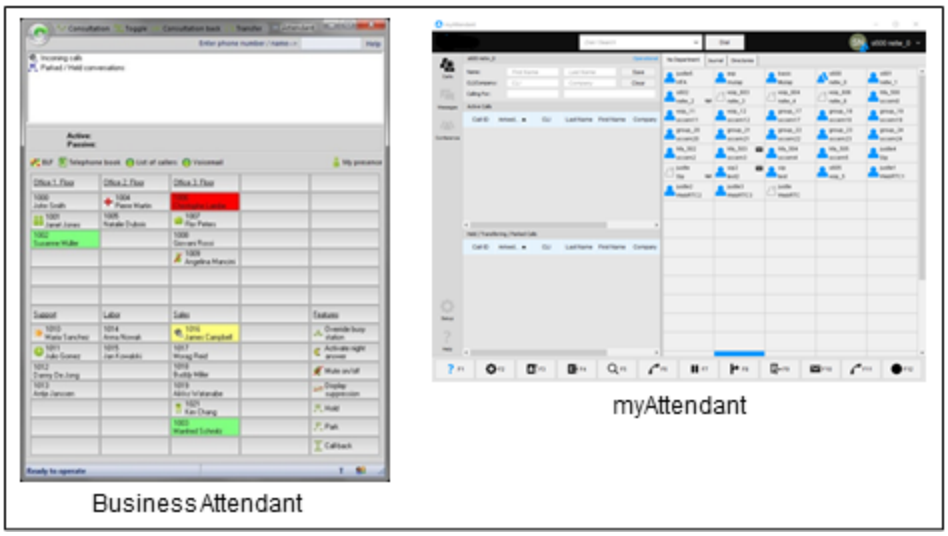


Figure 4: myAttendant

3.2.3 Integration in Business Applications

OpenScape Business can be integrated into existing IT infrastructures and business applications.

Applications

- Application Launcher for active interaction with CRM/ERP applications
- Accounting software for evaluating call charges

Integrated Services

- Directory services for information about callers and searching in internal and external directories
- Presence management and instant messaging (IM) to social media networks
- Web services for interactions with web-based applications on mobile phones and tablet PCs, for example

CTI Middleware

- First and third-party TAPI Service Provider for call control from CTI and CRM/ERP applications

Interfaces and Protocols

- CSTA for monitoring and controlling different applications
- SIP for connecting to SIP trunking based applications
- LDAP for connecting to external directories or from external LDAP clients
- HTTP and HTTPS for accessing UC functions of the integrated web server
- TCP/IP as the basic protocol for all Ethernet connections
- SQL connector for connecting SQL databases (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- LDAP connector for external LDAP servers such as Active Directory, for example

3.3 OpenScape Business Models

Different models are available for the use of telephony and UC functionality. You can choose between hardware models and pure software models that operate on standard servers or in a virtual environment with VMware vSphere.

The UC functionality for UC Smart is already integrated in OpenScape Business X. UC Suite additionally requires either the internally pluggable board "UC Booster Card" or the external Linux server "UC Booster Server". The OpenScape Business S softswitch optionally supports either UC Smart or UC Suite.

3.3.1 Expansion Levels Available through Sales

The OpenScape Business models have different expansion levels.

	X1	X3R/X3W	X5R/X5W	X8	S
Connection to Service Provider					
ITSP channels (SIP providers)	30	60	60	60	180
Max. number of active SIP providers	8	8	8	8	8

	X1	X3R/X3W	X5R/X5W	X8	S
ISDN S_0 (BRI)	4	20	52	128	-
	via mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	SW limit, i.e., regardless of the number of STDM3 boards	
ISDN S_{2M} (PRI)	-	30	30	120	-
			1* TS2	3 * DIUT3	
Max. number of trunk channels (ITSP, SIP-Q, Native SIP, TDM trunks, MEB)	250	250	250	250	250
Stations					
ISDN	4	20	52	128	-
	via mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analog	4	20	52/68	384	-
	via mainboard	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16* SLMA	
Digital ($U_{P0/E}$)	8	24	56	384	-
	via mainboard	2* SLU8(R)	6* SLU8(R)	16* SLMO2	
IP stations	20[1]	500	500	500	2000 (max. 500 SIP stations)
Cordless/DECT (CMI)	16	32	32/64	250	-
	1-7 base stations via Mainboard	1-7 base stations via mainboard + 8-15 via SLUN	1-7 base stations via mainboard + 8-15 via SLUN	4* SLMUC	
Max. number of stations	30[1]	500	500	500	2000
Unified Communications (UC Smart)					
UC Smart VoiceMail (Smart VM)	30	500/320[2]	500/320[2]	500/320[2]	1500
Maximum number of simultaneously active UC Smart clients (Sum of myPortal to go, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF and 3rd Party WSI Clients)	30	250/50[2]	250/50[2]	250/50[2]	250
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	250

	X1	X3R/X3W	X5R/X5W	X8	S
	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys
Max. number of the mobile stations	30	250/50[2]	250/50[2]	250/50[2]	250
Number of Mobility Entry User stations	30	150	150	150	250
myPortal to go	30	250/50[2]	250/50[2]	250/50[2]	250
myPortal for Teams	-	-	-	-	250
Maximum number of channels for UC conferences	30	30	30	30	60
Unified Communications (UC Suite)					
UC Suite VoiceMail	-	500	500	500	1500
Maximum number of simultaneously active UC Suite clients (Sum of myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent)	-	500/150[3]	500/150[3]	500/150[3]	1500
Max. number of other simultaneously active clients (Sum of myPortal to go, myPortal for Teams, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF and 3rd Party WSI Clients)	-	-	-	-	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 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys	Max 350 BLF keys
myAgent	-	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently	192 configurable / 64 active concurrently
Max. number of the mobile stations	-	250/150[3]	250/150[3]	250/150[3]	250
Number of Mobility Entry User stations	-	150	150	150	250
myPortal to go	-	250/100[3]	250/100[3]	250/100[3]	250
myPortal for Teams	-	-	-	-	250

	X1	X3R/X3W	X5R/X5W	X8	S
myReports	-	1	1	1	1
Max. number of simultaneous fax channels	-	8	8	8	8
Maximum number of Fax Users	-	500/150[3]	500/150[3]	500/150[3]	1500
Maximum number of channels for UC conferences	-	20	20	20	60
Unified Communications (CRM, database connectivity)					
Application Launcher	30 configurable / 30 active concurrently	500 configurable / 50 active concurrently	500 configurable / 50 active concurrently	500 configurable / 50 active concurrently	500
TAPI 120/170 User (via CSTA, UC Booster Server / Card required)	-	500/150[3]	500/150[3]	500/150[3]	1500
TAPI 120 User (in UC Smart mode via the mainboard without CSTA)	30	30	30	30	-
Directory Services Connector (UC Booster Card/Server required)	-	4	4	4	4

For a detailed description of the expansion levels and capacity limits, see also Configuration Limits and Capacities .

OpenScape Business UC Networking

OpenScape Business offers extensive network connectivity options:

- Extensive voice and UC networking between the various OpenScape Business X (UC Booster Card/Server required for UC networking) and OpenScape Business S
- with multiple buildings on the company premises
- with distributed locations
- Central administration, including licenses (HiPath 5000 RSM is no longer required)
- Voice networking with OpenScape Enterprise in preparation

Voice networking supports networks with up to 32 nodes. UC networking supports networks with up to 8 nodes and up to 1000 stations (1500 stations with OpenScape Business S). In addition, project-specific releases are possible.

For a detailed description of the networking scenarios, see Configuration Limits and Capacities .

1 Max. total number of IP and Deskshare Users = 20 (limited through configuration) - Max. total of IP, Deskshare, analog and digital stations = 30 (limited through licenses)
2 1st. value: maximum expansion with UC Booster Server / 2nd. value: maximum expansion with mainboard or UC Booster Card
3 1st. value: maximum expansion with UC Booster Server / 2nd. value: maximum expansion with UC Booster Card

3.3.2 UC Hardware Models

The OpenScape Business X communication systems offer a high degree of flexibility in terms of functionality and design. Depending on the OpenScape Business X model, up to 500 stations are supported for IP, digital (ISDN), analog (a/b) and Cordless (DECT), and connections to the public network using ITSP (SIP), ISDN (BRI and PRI), CAS and analog and onboard IP (provisioned on the mainboard).

- OpenScape Business X1W

  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X1R

  Communication system which comes in a 19-inch rack housing and can be installed in a 19-inch rack, as a standalone unit (desktop operation) or wall mounted.
- OpenScape Business X3W

  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X3R

  Communication system which comes in a 19-inch rack housing and can be installed in a 19-inch rack, as a standalone unit (desktop operation) or wall mounted.
- OpenScape Business X5 W

  Communication system which comes in a wall housing and must be wall mounted.
- OpenScape Business X5R

  Communication system which comes in a 19-inch rack housing and can be installed in a 19-inch rack, as a standalone unit (desktop operation) or wall mounted.
- OpenScape Business X8

  Modular communication system which can be used as a one-box system (base box) or two-box system (base box + expansion box). The communication system can be installed as a standalone unit or mounted in a 19-inch rack.



Figure 5: Hardware Platforms

3.3.3 UC Booster Hardware

UC Booster Hardware for OpenScape Business X.

- OpenScape Business UC Booster Card

  Board for OpenScape Business X if UC Suite is to be used as a UC solution with up to 150 UC users.
- OpenScape Business UC Booster Server

  External UC Booster Server (Linux) for OpenScape Business X if UC Suite is to be used as a UC solution with up to 500 UC users.

  SLES 12 SP5 64-bit or SLES 15 SP6 64-bit is used on the UC Booster Server. The UC Booster Server can also be run in a virtual environment with VMware vSphere.

  When using the UC Booster Server, the UC Booster Card is not required.
- OpenScape Business Voice Channel Booster Card

  Two optional modules for the extension of OpenScape Business X with additional DSP channels (e.g., for simultaneous voice connections with IP/TDM transitions).

  Eight DSP channels are provided on the mainboard. The Voice Channel Booster Card OCCB/1 provides a further 48 DSP channels, and the Voice Channel Booster Card OCCB/3 provides up to 128 DSP channels.

3.3.4 UC Software Models (Softswitch)

All-in-one server-based UC software solution that supports up to 1000 IP stations with connections to the public network using ITSP (SIP).

Independent of the platform used, OpenScape Business S can be installed on a Linux server. SLES 12 SP5 64 bit or SLES 15 SP6 64-bit, are used as operating systems. OpenScape Business S can also be run in a virtual environment with VMware vSphere. If TDM interfaces are required for connection to TDM telephones or TDM trunks, OpenScape Business X systems can be used as a gateway.

3.3.5 Structure and Environmental Conditions

	X1	X1R	X3W	X3R	X5W	X5R	X8
Structure	Wall-mount system	Rack	Wall-mount system	Rack	Wall-mount system	Rack	Standard system (rack installation also possible)
Dimensions (HxBxT in mm)	470x370x80	450x460x130	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Weight	about 2.8 kg	about 6 kg	about 6 kg	about 6 kg	about 8 kg	about 8 kg	about 34 kg (fully loaded)
Housing color	White	Black	White	Green / Dark Grey	White	Green / Dark Grey	Green / Dark Grey

	X1	X1R	X3W	X3R	X5W	X5R	X8
Power supply	The models are equipped for connection to the power supply. • Rated input voltage (AC): 100 to 240 V • Nominal frequency: 50/60 Hz • Battery power (DC): -48 V						
Power consumption	Depending on the hardware platform and expansion						
Environmental Conditions	• Operating conditions: +5 to +40 °C (41 to 104 °F) • Humidity: 5 to 85%						

3.3.6 Supported Phones

OpenScape Business X enables telephony over IP/HFA (HiPath Feature Access), SIP, TDM, a/b, Cordless/DECT and WLAN. IP/HFA, SIP and wireless phones can be connected to OpenScape Business S.

OpenStage telephones (IP/HFA, SIP and T)	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/HFA, SIP, and T)	• OpenScape Desk Phone IP 35G/55G/35G Eco • OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA and SIP 200/400/205/405 TDM • OpenScape Desk Phone CP 110/210/410/710 HFA and SIP
Key modules	• OpenStage Key Module, only for OpenStage 15/40/60 • OpenStage BLF 40 (Busy Lamp Field), only for OpenStage 40 and OpenStage 30 T • OpenScape Key Module 400/600, only for CP 400/600/600E/700/700X • OpenScape Key Module 410/710, only for CP 710
OpenScape Business Cordless	• OpenStage M3 • OpenScape DECT Phone S6/SL6/R6
PC clients (HFA, SIP)	• OpenScape Personal Edition (incl. video for SIP)
SIP phones (UC Suite) / AP adapter	• SIP phones with RFC 3725 support • Mediatrix 4102S (for connecting 2 analog phones or Fax devices)

WLAN Phones	• OpenStage WL3 professional • OpenScape WLAN Phone WL4/WL4 Plus
Analog and ISDN phones	• Analog (a/b) phones • Digital (S_0) ISDN phones

Older devices (such as optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 and optiPoint WL2 SIP) are supported. Optiset E devices cannot be operated.

Functions and Configuration of SIP Phones

OpenScape Business offers an extensive range of voice communication features for OpenStage HFA telephones. Many functions are also available for standard SIP phones.

An overview of the features supported with OpenStage SIP telephones and further information can be found in the Unify wiki at the following link

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

To control voice calls for SIP telephones using CTI (3PCC), a UC Booster Card or a UC Booster Server is required for OpenScape Business X3/X5/X8.

The control of voice calls for SIP telephones via UC Smart clients is supported for the OpenScape Business X3/X5 rack models with the Booster Card.

With the help of the DLI functions, the OpenScape Desk Phone (SIP) telephones can be centrally administered and supplied with software.

Related concepts
CSTA on page 1104

3.4 Further information

Further information can be found on the Internet and extranet. See also the release notes for limitations and recent changes.

3.4.1 Languages Supported

Several different language variants are available for the various software components (clients and WBM) and documentation/online help.

The following languages will be released as part of the country-specific introduction.

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
UC Smart Clients										

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (User Guide)	X	X	X	X	X	X	X	-	-	-
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Quick Reference Guide)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (Client)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (User Guide)	X	X	–	–	–	X	–	–	–	–
UC Suite Clients										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (User Guide)	X	X	X	X	X	X	X	-	-	-
myPortal for Desktop (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (User Guide/Online Help)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (User Guide/Online Help)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X
TUI (Quick Reference Guide)	X	X	–	–	–	–	–	–	–	–
Administration										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
OpenScape Business Assistant (Administrator Documentation/Online Help)	X	X (no nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Administrator Documentation/ Online Help)	X	X	–	–	X	–	–	–	–	–

In addition, the UC Smart TUI is also offered in the languages Belgian (Flemish) and Slovenian.

INFO: A Russian or Chinese Windows operating system is required in order to use the Russian or Chinese user interface.

The following language codes (ISO 639-1) are used for the abbreviations in the table:

- de = German
- en = English
- cs = Czech
- da = Danish
- es = Spanish
- fi = Finnish
- fr = French
- hr = Croatian
- hu = Hungarian
- it = Italian
- nl = Dutch
- no = Norwegian
- pl = Polish
- pt = Portuguese
- ru = Russian
- sv = Swedish
- tr = Turkish
- zh = Chinese

3.4.2 Internet Links

More details and possibly more up-to-date information can be found on the Unify homepage, our expert wiki and the Unify portal for partners.

Internet Links

- Unify homepage:

  `http://www.unify.com`
- Expert wiki for telephones, communication systems and UC:

  `http://wiki.unify.com`
- Partner Portal (registration required):

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

  or

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

4 Administration Concept

The administration of the communication system is performed with the OpenScape Business Assistant.

4.1 OpenScape Business Assistant (WBM)

The OpenScape Business Assistant is web-based and is therefore also called Web-Based Management (WBM).

The scope of administrative tasks offered depends on the administrator profile being used.

An online help is available for each page of the WBM.

4.1.1 Requirements for the WBM

In order to use the WBM, the administration PC must have the appropriate software installed.

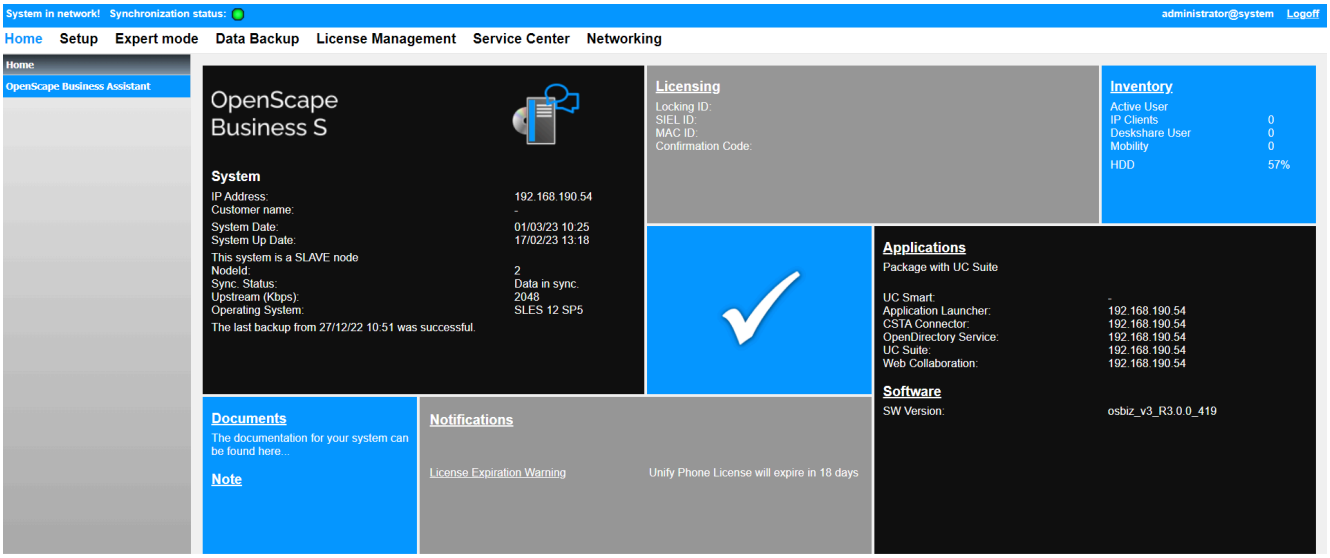
Supported Web browsers:

- Microsoft Internet Explorer 10 or later
- Microsoft Edge
- Mozilla Firefox 18 or later
- Google Chrome

4.1.2 Home Page of the WBM

The home page of WBM displays important system information, which is split into different areas (tiles). In addition, it includes notes and provides information on system errors, events and actions.

The presented system information depends on the administrator profile being used. The underlined headings in the individual areas are clickable and reference the related topic in the WBM.



The following information is displayed:

- Area: **Status** (Middle)
  - White check mark on blue background: the communication system is fully functional - Messages highlighted in red in the other fields indicate actions that should be performed.
  - White exclamation mark on red background: the communication system is not fully functional and requires the intervention of the administrator - Messages highlighted in red in the other fields indicate system errors or events that need to be resolved.
- Area: **System**
  - Brand
  - IP address of the communication system
  - Current date and time
  - Date and time of the last system restart
  - Notes when operating in an internetwork (system is master or slave, display of node ID)
  - Synchronization status
  - Bandwidth Upstream in kbps
  - SDHC Health Status
  - Notes on performing a backup and restore
  - Booster Card status
- Area: **Documents**
  - Link to the documentation
- Area: **Notifications**
  - Various notifications about the system
- Area: **Note**
  - Displays the latest information entered by an administrator. Clicking on the underlined title opens a text window in which all the information is displayed and further information can be entered.

    Data of the Note field are not included in the backup set of the system. Consequently, when restoring a back up set these data will not be restored.

- Area: **Licensing**
  - Locking ID for licensing
  - SIEL ID for licensing
  - Note on the licensing status, indicating if the system is in "Permanent" license mode or in "Pay As You Go" mode.
- Area: **Inventory**
  - Type and number of active stations
  - Number of activated ITSPs and a link to the ITSP status dialog in Service Center of active stations
- Area: **Applications** and Software

  Applications:
  - Used application package (UC Smart or UC Suite) and its components, including the IP addresses of the servers used.
  - Indicates whether a UC Booster Card is inserted.

  Software:
  - Version of the installed communication system software
  - Indicates whether a UC Booster Card is inserted. If the Booster Card is additionally accessible via an IP address, the version of the installed UC Booster Card software is displayed.

    The UC Booster Card and the communication system should always be on the same software version.
  - Expiration date of the 3-year software support.

    After the expiration date the message "Software Support licence has been expired, please update the Software Support licence" is displayed.
  - Note on the new software version

4.1.3 Introduction to the WBM

WBM is the web-based application for the administration of the system.

Language of the User Interface

You can select one of the following languages at login:

- German
- English
- French
- Italian
- Dutch (The online help is only available in English)
- Portuguese
- Spanish

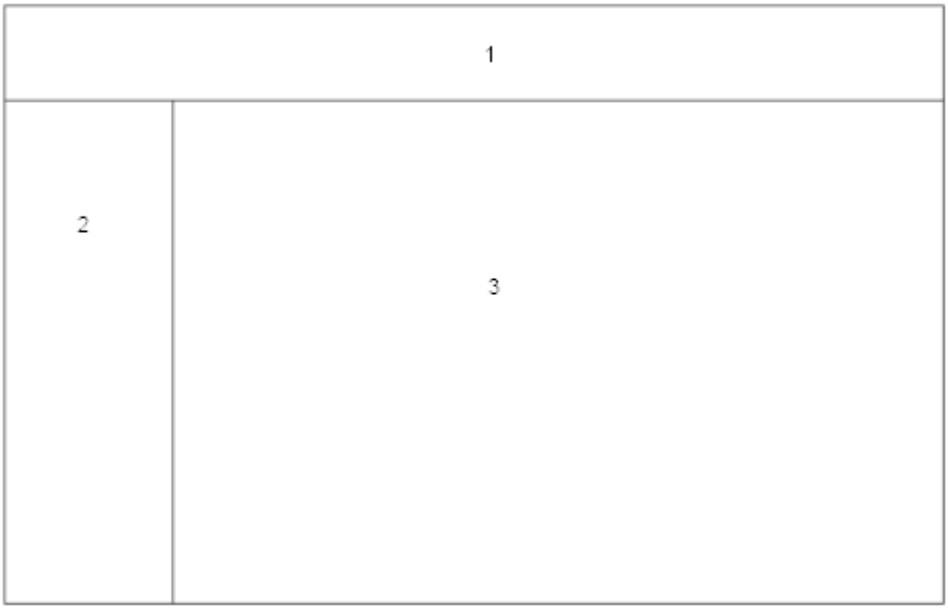
Ranking of the User Interfaces Described

Any tasks which can be performed in a wizard are described for the corresponding wizard only.

Any additional tasks which can be performed in Expert mode are described for the Expert mode only.

Any other remaining tasks are described for E Manager.

User Interface Elements



- Navigation bar (1)

  The navigation is the primary navigation aid and always shows the same links to main task centers, i.e., **Home**, **Administrators**, **Setup**, **Expert Mode**, **Data Backup**, **License Management**, **Service Center** as well as the current user name and the **Logout** link. When you click on one of these task centers, the associated navigation tree opens in the navigation area, and the home page of the task center appears in the workspace.
- Navigation area (2)

  The navigation area is the secondary aid and contains the navigation tree with the menu items of the selected task center. The name of the selected task center is displayed at the top of the navigation tree with expandable and collapsible menu groups and menu items below it. Different menu items are displayed in the menu groups, depending on the situation. Clicking on a menu item displays the associated page in the workspace.
- Workspace (3)

  The workspace is where administration tasks are performed. It is usually opened in a separate window. The number and selection of messages and actions displayed depends on the menu item selected in the navigation tree. In Expert mode, the menu tree is displayed on the left in the workspace.

Navigating in the Menu Tree

The menu tree is used for navigation in the Expert mode of the WBM. The menu tree contains folders (e.g., **Maintenance**) with further elements (e.g., **Restart / Reload**).

You can navigate in the menu tree by clicking on a folder (which toggles its expanded or collapsed state).

Automatic Logout After Timeout

You are automatically logged off after 30 minutes of inactivity. You must log in again to continue working with the WBM. If you make some changes and then take a break, to be on the safe side, you should reload the page before making any further changes so that no changes are lost due the automatic logout.

4.1.3.1 How to Log into the WBM

Prerequisites

Your must have access to your user credentials (user name and password). If not, obtain this from your administrator.

TLS 1.2 is enabled in your web browser settings.

Step by Step

1) Open the login page in your web browser by entering the following address: `https://<IP address of communication system>`. The default IP address is 192.168.1.2.
2) Click on the language code at the top right and select the language in which the user interface of the WBM is to be displayed from the menu. The Login page will be displayed in the selected language.
3) Enter the user name under **Login** in the first field. "@system" is added automatically on exiting the field.
4) Enter your password in the second field under **Login**. Note case usage and the status of the **Num** key. The password is shown with asterisks (*).
5) Click **Login**.

If you enter invalid credentials, a message is displayed after the third failed login attempt, informing you that the account is blocked for 5 minutes. You can try to login again after this time period.

For any further failed login attempt, this time period is doubled reaching 160 minutes in the eighth failed attempt. For every consequent failed attempt the account blocking time is 160 minutes.

4.1.3.2 How to Log out from the WBM

Procedure

- Click **Logout** at the top right of the screen.

4.1.4 WBM User Management

You can configure and manage up to 16 administrators for WBM (web-based management). Every administrator is assigned a profile that specifies the scope of his or her authorization. You can also change the password of a Manager E administrator.

The users of WBM are also referred to as administrators.

The default Administrator is `administrator@system` with the default password `administrator` and has the profile **Advanced**. This password must be changed on logging in for the first time. The password for an administrator must consist of at least 8 characters and a maximum of 128 characters, of which at least one character must be a digit. In addition, for a secure password, at least an uppercase letter, one lowercase letter and one special character should be included in the password.

NOTICE: Administrative access (including admin user role) is logged to the messages log file/syslog. It can be accessed via the **Diagnostics** > **Trace** menu.

Profiles

The WBM supports four profiles with different classes of service (authorizations) for administrators with different levels of technical expertise and tasks.

In order to prevent that no malicious user could login via ISDN and change the default password when logging in for the first time, it is compulsory for the user to change the password via Manager E as an installation step.

NOTICE: A password, which consists of 5 characters (*****), will not be accepted by the system for security reasons.

Table 1: Profile Classes of Service

Profile	Class of Service
Basic Basic knowledge of configuring the system	System information on the home page **Key Programming** wizard **Phone Book / Speed Dialing** wizard **Call Detail Recording** wizard **Music on Hold / Announcements** wizard **Station name and release** wizard Access to **Administrators** (only to change their own passwords) Access to **License Management** > **License Information** Access to **Service Center** > **Documents** Access to **Service Center** > **Software**

Profile	Class of Service
Enhanced Good knowledge of configuring the system	As for the **Basic** profile, plus: Access to all wizards (except the **Basic Installation**, **UC Suite** and **UC Smart** wizards) **NOTICE:** Access to all wizards is not supported in OpenScape Business S systems. Access to **Administrators** (only to change their own passwords) Access to **Backup And Restore** Access to **License Management** (excluding registration, license activation and settings) Access to **Service Center** > **Inventory** Access to **Service Center** > **Restart / Reload** (without reload) Access to **Service Center** > **Diagnostics** > **Status** Access to **Service Center** > **Diagnostics** > **Event Viewer**
Advanced Trained users	As for the **Enhanced** profile, plus: Access to all wizards Access to **Administrators** (only to change their own passwords) Access to the complete **License Management** Access to the complete **Service Center** Access to **Networking**
Expert Trained service technicians	As for the **Advanced** profile, plus: Access to **Administrators** (complete) Access to the **Expert mode**

Table 2: Profile Management

Profile	Maintenance
Basic Basic knowledge of configuring the system	Can change own password. Does not see any other configured administrators except himself or herself.
Enhanced Good knowledge of configuring the system	Can change own password. Does not see any other configured administrators except himself or herself.

Profile	Maintenance
Advanced Trained users	Can change own password. Does not see any other configured administrators except himself or herself.
Expert Trained service technicians	Can change own password and the user names and passwords of other administrators. Sees all configured administrators. Can add, edit and remove administrators.

NOTICE: As long as no administrator with the **Expert** profile exists, administrators with the **Advanced** profile can add, edit and remove further administrators. As soon as an administrator with the **Expert** profile exists, only administrators with the **Expert** profile can add, edit and remove further administrators.

Administrator Management in the Internetwork

The direct management of administrators is only possible in the WBM of the master node. The **Administrator** menu is not displayed on slave nodes. All administrator configurations are transmitted to the slave nodes. It is, however, possible to call up the WBM of the master node from within the WBM of the slave node via the Node View. The **Administrator** menu is displayed here, and administrators can only be displayed.

NOTICE: The Add/Edit/Delete of the users is not possible via slave mode WBM access (but only via Master mode WBM access).

Manager E Password Administration

An administrator can change (but not create a new user role) the password of the existing users which can access the embedded system through Manager E.

User will be prompted to change passwords only for the existing users and will not be able to change the user's Group and options like Created, Last Used are not viewable. This is a security feature and thus it does not provide the whole Manager E's administration screen.

4.1.4.1 How to Add an Administrator

Prerequisites

You are logged on to the WBM with the **Advanced** profile. (As long as no administrator with the **Expert** profile exists.)

You are logged into the WBM with the **Expert** profile. (If an administrator with the **Expert** profile already exists.)

Step by Step

1) Click on **Administrators** in the navigation bar.

2) Click on **Add...**.
3) Enter the following data: **Login Name**, **First Name**, **Last Name**, **Password**, **Retype Password**.
4) Select the desired user profile from the **User Role** drop-down list.
5) Click on **OK & Next**.

4.1.4.2 How to Edit an Administrator

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Click on **Administrators** in the navigation bar.
2) Select the check box for the desired administrator in the **Administrators List**.
3) Click on **Edit**.
4) Edit the data (login name, first name and last name, password, and user role) as required.
5) Click **OK & Next**.

4.1.4.3 How to Change your Own Administrator Password

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Click on **Administrators** in the navigation bar.
2) Enter the new password in the **Password** and **Retype Password** fields.

> **NOTICE:** A password, which consists of 5 stars (*****), will not be accepted by the system for security reasons.

3) Click **OK & Next**.

Related concepts

Immediate Backup on page 1184

4.1.4.4 How to Delete an Administrator

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Click on **Administrators** in the navigation bar.

2) Select the check box for the relevant administrator in the relevant **Administrators List**.
3) Click on **Delete...**.

4.1.4.5 How to change a Manager E Administrator password

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Click on **Administrators** in the navigation bar.
2) Click on Manager E **AdministratorsList**.
3) Edit the data (User Accounts, New Password, Confirm Password) as required.
4) Click on **Save**.

NOTICE: The password must consist of at least 5 digits. The use of letters or other characters is not allowed. Also, old passwords cannot be reused.

4.1.5 Wizards

Wizards make it easy to install and configure the system. Only selected subset of the wizards are available to a customer administrator (with the **Basic** profile). A trained service technician or an administrator with expertise (with the **Advanced** profile), by contrast, can access all the wizards.

The available wizards depend on the system configuration (UC Smart or UC Suite). Wizards can consist of several pages in succession. OK & Next saves changes and switches to the next page in the wizard. There is no undo function for changes committed with OK & Next. If no changes were saved, **Abort** closes the wizard. Clicking the **X** symbol in the upper right corner of the wizard window terminates the wizard and retains the changes previously saved with OK & Next.

4.1.5.1 Wizards – Basic Installation

The wizards under **Basic Installation** support the simple basic installation.

The following wizards are available under **Basic Installation**:

- **Initial installation**

  Single usage at initial setup. Country initialization, System IP address and DHCP server.
- **Basic Installation**

  Basic setup of system with station data, trunks, network parameters and Internet.

- **Licensing**

  Activating licenses online via the License Server.
- **Networking Configuration**

  Setup of system as part of a network.
- **Power Management**

  Setup and Activation of Power Management

4.1.5.2 Wizards – Network / Internet

The wizards under **Network / Internet** support the simple configuration of networks and the Internet access.

The following wizards are available under **Network / Internet**:

- **Network Configuration**

  Set up DHCP, IP Routing and DNS Server.
- **Internet Configuration**

  Access parameters of the Internet Provider data, e.g., User Account and Password.
- **VPN Configuration**

  Connection of workplaces via the Internet.

4.1.5.3 Wizards – Telephones / Subscribers

The wizards under **Telephones / Subscribers** support the simple configuration of phones and subscribers.

The following wizards are available under **Telephones / Subscribers**:

- **IP devices**

  Set up system-specific IP and SIP telephones, FAX call numbers as well as IP/analog adapters.
- **UP0 devices**

  Set up UP0 Telephones, FAX call numbers.
- **DECT phones**

  Set up DECT phone, FAX call numbers.
- **Mitel SIP DECT**

  Configuration of Mitel SIP DECT RFP Devices.
- **ISDN devices**

  Unpowered ISDN ports for ISDN cards / modems and S0 stations.
- **Analog Terminals**

  Analog DTMF and CLIP-capable ports for Fax and Telephone.
- **Key programming**

  Name and function key programming for system-specific IP devices and UP0 telephones.

4.1.5.4 Wizards – Central Telephony

The wizards under **Central Telephony** support the simple configuration of central telephony features.

The following wizards are available under **Central Telephony**:

- **CO Trunk ISDN / Analog / ITSP**

  Point-to-multipoint connections (MSN) and PABX number for ISDN connections, and assignment of analog and ITSP trunks.
- **Internet Telephony**

  Access parameters of the Internet Telephony Service Provider (ITSP), e.g., user account, password, SIP station number.
- **Phone book / Speed Dialing**

  Set up central speed-dial destinations for the system's internal phone book.
- **Call Detail Recording**

  Set up call detail recording connection parameters for call detail applications.
- **Music on Hold / Announcements**

  Record new melodies and announcements for Music on Hold and announcement before answering.
- **Entrance Telephone (Door Opener)**

  Set up call allocation and access authorization for the entrance telephone at the analog station connection.
- **SmartVM**

  Setup of the UC Smart voicemail box (SmartVM).
- **Blacklist for incoming calls**

  Define a list of numbers to block unwanted callers permanently.
- **Active Directory Integration Service**

  Set up the Active Directory.

4.1.5.5 Wizards – User Telephony

The wizards under **User Telephony** support the simple configuration of user telephony features.

The following wizards are available under **User Telephony**:

- **Class of Service**

  Set up classes of service with external call numbers that can be assigned to subscribers, e.g., emergency numbers, allowed numbers, denied numbers and assignment of class of service for night service.
- **Station Name and Release**

  Edit station and group names and reset lock code for individual stations.
- **Group call / Hunt group**

  Set up incoming calls for station groups (parallel, linear or cyclical call order).
- **Call Forwarding**

  Set up central system-wide station number assignments, and forwarding "after timeout" and "on busy".

- **Call pickup**

  Configure stations in a pickup group with the option of answering each other's calls.
- **Team Configuration**

  Setting up stations which are called concurrently with the main station for incoming calls and which can use its station number for outgoing calls.
- **Mobile Phone Integration**

  Set up a link between a mobile phone and an internal station with the goal of enabling incoming and outgoing availability under one station number (One Number Service).
- **Executive / Secretary**

  Set up a link between one or more Executive phones and one or more Secretary phones with the goal of enabling simplified call transfers and ring transfers.
- **UCD**

  Set up an automatic intelligent call distribution to a group with selected stations.
- **Attendant Console**

  Set up stations as attendant console numbers and station behavior for on busy, incorrect dialing and no answer.
- **Station Profiles**

  Assign stations to a profile and import/export profile data.

4.1.5.6 Wizards – Security

The wizards under **Security** support the simple configuration of the firewall.

The following wizards are available under **Security**:

- **Firewall**

  Configure port opening to restrict Internet traffic.

4.1.5.7 Wizards - UC Smart (only with UC Smart)

The setup of the UC solution UC Smart is supported by wizards under **UC Suite**.

The following wizards are available under **UC Smart** :

- **UC Smart**

  Basic Setup and User Configuration for UC Smart.

4.1.5.8 Wizards - UC Suite (only with UC Suite)

The setup of the UC solution UC Suite is supported by wizards under **UC Suite**.

The following wizards are available under **UC Suite**:

- **User Directory**

  Configuration of users.
- **Departments**

  Configuration of departments.
- **Groups**

  Configuration of voicemail and fax groups.
- **Templates**

  Configuration of SMS templates.
- **External Directory**

  Manual addition of individual contacts to the external directory.
- **External Providers Config**

  Input of access data for the Exchange or LDAP server.
- **Contact Center**

  Configuration of the Contact Center.
- **Schedules**

  Configuration of schedules.
- **File Upload**

  Uploading of audio files for announcements and music on hold.
- **Conferencing**

  Configuration of conference calls.
- **Profiles**

  Creation of user profiles.
- **Fax Headlines**

  Configuration of fax headers.

4.1.5.9 Wizards – Unified Directory

The wizards under **Unified Directory** support the importing and editing of directory contacts.

The following wizards are available under **Unified Directory**:

- **Import Contacts**

  The Wizard will guide you through the import of contact data to the Global Directory from CSV.
- **Edit Contacts**

  Manually add or edit Global Directory entries.

4.1.5.10 Wizards - Cloud Services

The wizards under **Cloud Services** support functionality supported in the cloud.

The following wizards are available under **Cloud Services**:

- **Microsoft Teams Client-Plugin**

  Configure and download myPortal for Teams client plugin.

- **Unify Phone Connectivity**

  Basic settings configuration for Unify Phone.
- **Unify Phone user instance**

  Configure Unify Phone users instance
- **Let's Encrypt Service**

  Configure the Let's Encrypt Service
- **CloudLink Service**

  Configure the CloudLink Service
- **CloudLink Pilot Numbers**

  Configure Pilot Numbers for CloudLink

4.1.6 Service Center

The **Service Center** of the WBM offers various maintenance functions, starts the software update and makes the documentation and software available.

4.1.6.1 Service Center – Documents

The **Documents** option provides documentation, CSV templates and links to related information. The documentation can be accessed in all the supported languages in PDF format.

Depending on the system configuration, the following contents are available:

Contents	UC Smart	UC Suite
Administrator Documentation (PDF)	-	x
User Documentation (PDF)	-	x
Links (Wiki)	x	x
Templates (CSV Templates) for importing data for • Stations • System Speed Dialing • External directory	x	x
EULA	x	x

Related concepts

Accounting Tools on page 1166

4.1.6.2 Service Center – Software

The **Software** option provides the software for the UC clients, USB drivers and tools.

The following contents are available:

Contents	UC Smart	UC Suite
Installation files for the software of the UC clients	x	x
USB drivers	x	x
Tools	x	x
Links for direct access to the installation files	-	x

4.1.6.3 Service Center – Inventory > System

System provides an overview of the basic configuration data of the system.

4.1.6.4 Service Center – Inventory > Call Numbers

Call Numbers provides a list of all assigned call numbers.

4.1.6.5 Service Center – Inventory > Network Overview

Network Overview provides a list with information about the systems currently in the network.

4.1.6.6 Service Center – Software Update

Software Update checks whether a software update is available on the web server and performs the update.

4.1.6.7 Service Center – E-mail Forwarding

E-mail Forwarding enables the sending of e-mails with system messages from the UC Suite to the administrator and e-mails with attached voicemail of fax messages to subscribers.

4.1.6.8 Service Center – Remote Access

Remote Access is used to configure access for the site-independent administration of the system.

4.1.6.9 Service Center – Restart / Reload

Restart / Reload enables a restart of the system, optionally resetting it back to factory settings.

4.1.6.10 Service Center – Diagnostics > Status

Status provides status information on the network, subscribers, call setup, ITSP and VPN.

See also Inventory Management .

4.1.6.11 Service Center – Diagnostics > Event Viewer

Event Viewer logs system events.

See also Traces .

4.1.6.12 Service Center – Diagnostics > Trace

Trace provides options for fault logging.

See also Traces .

4.1.6.13 Service Center – Diagnostics > Service log

Service log logs several system data in the form of HiPath 3000 Event.

It is necessary to be on WBM View mode, to refresh or download the file.

4.1.7 Expert Mode

The Expert mode provides trained service technicians (**Expert** profile) with several menus and functions to configure and maintain the system.

Detailed information can be found in the section on Expert mode.

4.1.8 Online Help

The integrated online help describes key concepts and operating instructions. The online help is context-sensitive and opens the associated Help topic for each opened WBM page.

Navigation

The buttons in the online help provide the following functions:

- **Contents**

  provides you with an overview of the structure
- **Index**

  provides direct access to a topic using keywords
- **Search**

  allows you to do a full-text search and selectively find all relevant topics

4.1.8.1 How to Invoke the Context-Sensitive Online Help

Prerequisites

You are logged in at the WBM.

Procedure

- Click in the open WBM window on either the question mark icon at the top right or the Help button at the bottom left.

4.2 Manager E

Manager E is a service tool with integrated help that runs under Windows and can be used for tasks which cannot be performed via the WBM.

Manager E can be used for OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 and OpenScape Business X8. OpenScape Business S cannot be administered using Manager E.

It is advisable to make configuration changes via Manager E only when you cannot perform them via WBM, for example, attenuation, ring pulse, tone frequency etc. Changes done via Manager E must be sent via delta mode.

Manager E is intended for trained service personnel and includes the following function blocks:

- Generation (including off-line generation)
- Copying and backing up customer data
- Service orders, such as restarting boards
- Resetting activated features
- Creation and printing of:
  - Key labels for optiPoint 500
  - Customer data printouts
  - Main distribution frame layout
- Separate user and password administration for after sales service.
- Database conversion routine for customer database (CDB).

System access via Manager requires a user name and a password. The Online mode can be used to perform changes quickly. The functionality of the Online mode corresponds to the Assistant T user interface.

The following features can no longer be administered using Manager E:

- Licensing
- Network
  - SNMP Partner
  - PSTN Peer
  - Routing
  - Mapping
  - Gatekeeper
  - Ext. H.323
  - IP Ports

- Maintenance
  - Error History
  - Event Log
  - Trace settings
  - Error Reaction Table
  - V.24 Status
  - DMA
- Traces

Working with the Customer Database (CDB)

The basic steps are as follows:

- Load the CDB from the system into Manager E
- Make any necessary changes in E Manager
- Use Manager E to store the CDB back on the system

4.2.1 How to Load the CDB into Manager E

Perform the following steps, and then proceed to perform configuration tasks in E Manager.

Step by Step

1) Start Manager E on the admin PC.
2) Enter the **User name** for Manager E.
3) Enter the **Password** for Manager E.
4) Click on **File** > **Transfer**.
5) Click on the **Communications** tab.
6) Select the appropriate option in the **Access** area, depending on the type of connection from the admin PC to the communication system.
7) Activate the **Read/write database** option.
8) Click on **System -> PC**.
9) Click on **OK**. The CDB is transferred from the system to Manager E.
10) Click **OK** once the transfer has been successfully completed.
11) Click on **Close**.

4.2.2 How to Load the CDB Back into the System

The configuration saved in Manager E can be loaded back into the system by performing the following steps:

Step by Step

1) Click on **File** > **Transfer**.
2) Click on the **Communications** tab.
3) Select the appropriate option in the **Access** area, depending on the type of connection from the admin PC to the communication system.
4) Activate the **Read/write database** option.

5) Click on **PC -> system**.
6) Click on **OK**. The CDB is transferred from Manager E to the sytem.
7) Click **OK** once the transfer has been successfully completed.
8) Click on **Close**.

5 Initial Setup for OpenScape Business X

This chapter describes the initial setup of OpenScape Business X1/X3/X5/X8. The communication system and its components are integrated into an existing infrastructure consisting of a customer LAN and a TDM telephony network. Internet access and the trunk connection are set up and the connected stations are configured.

The initial setup of OpenScape Business X1/X3/X5/X8 (i.e., the communication system) is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM).

The standard initial setup of commonly used components is described here. The specific installation steps depend on the communication system and the components (e.g., the UC Booster Card) involved. During the initial setup, you may need to choose between multiple options in some places or even skip some configurations entirely. It is also possible that the installation steps described here do not appear in your communication system.

The detailed configurations of features not covered by the standard initial setup are described in subsequent chapters.

The initial setup requires the creation of an IP address scheme and a dial plan.

The most important installation steps are as follows:

- IP addresses and DHCP settings
- Country and Time Settings
- System Phone Numbers and Networking
- ISDN Configuration
- Internet access
- Internet telephony
- Station configuration
- Licensing
- System hardening
- Data backup

Before implementing these changes, consider the following:

Ensure the following networks do not overlap with other system networks. Specifically:

- DSP network
- LAN1 (WAN) network
- LAN2 network
- LAN3 (Admin) network

Additionally, ensure that there are no conflicts with the default gateway IP address. If a Booster card is present, the system’s LAN2 interface must be configured within the same subnet as the Booster card’s LAN2 interface.

5.1 Prerequisites for the Initial installation

Meeting the prerequisites for the initial installation ensures the proper operation of the communication system.

General

Depending on the existing hardware (boards, phones, ...) and infrastructure, the following general conditions apply:

- The infrastructure (LAN, TDM telephony network) is available and usable.
- The hardware is installed and connected properly.
- One LAN port each is required to integrate the mainboard and the UC Booster Card in the customer LAN.
- The communication system has not yet been connected to the LAN.
- If the UC Booster Card is used, it should be inserted prior to the initial installation.
- Internet access is available through an Internet Service Provider.
- An ISDN S_0 or ISDN Primary Rate Interface is required for using ISDN outside lines.
- A CAS trunk connection is required for using a CAS outside line.
- An analog trunk connection is required for using an analog outside line.
- An IP address scheme exists and is known (see IP Address Scheme).
- A dial plan (also called a numbering plan) is present and known (see Dial Plan).

Admin PC

The following prerequisites must be fulfilled for the Administration PC (Admin PC) that is used for initially setting up the system and for the subsequent administration of the communication system:

- Network interface:

  The admin PC requires an available LAN port.
- Operating system:

  Configuring the communication system with the Manager E is only possible on a Windows operating system (Windows XP and later).

  WBM configuration, however, is browser-based and therefore platform-independent.
- Web browser:

  The following web browsers are supported:

  – Microsoft Internet Explorer Version 10 and later.
  – Microsoft Edge
  – Mozilla Firefox Version 17 and later.
  – Google Chrome

  If an older version of the Web browser is installed, you will need to install an up-to-date version before you can start setting up the system.
- Java:

  Oracle Java 8 or higher or alternatively OpenJDK 8 must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system.

5.2 Components

The various components of the installation example are described and outlined below.

The installation example includes the following components:

- OpenScape Business X

  The communication system is integrated in the existing customer LAN via the LAN interface.
- Admin PC

  The admin PC is also connected to the communication system via a LAN interface.
- IP stations (IP clients)

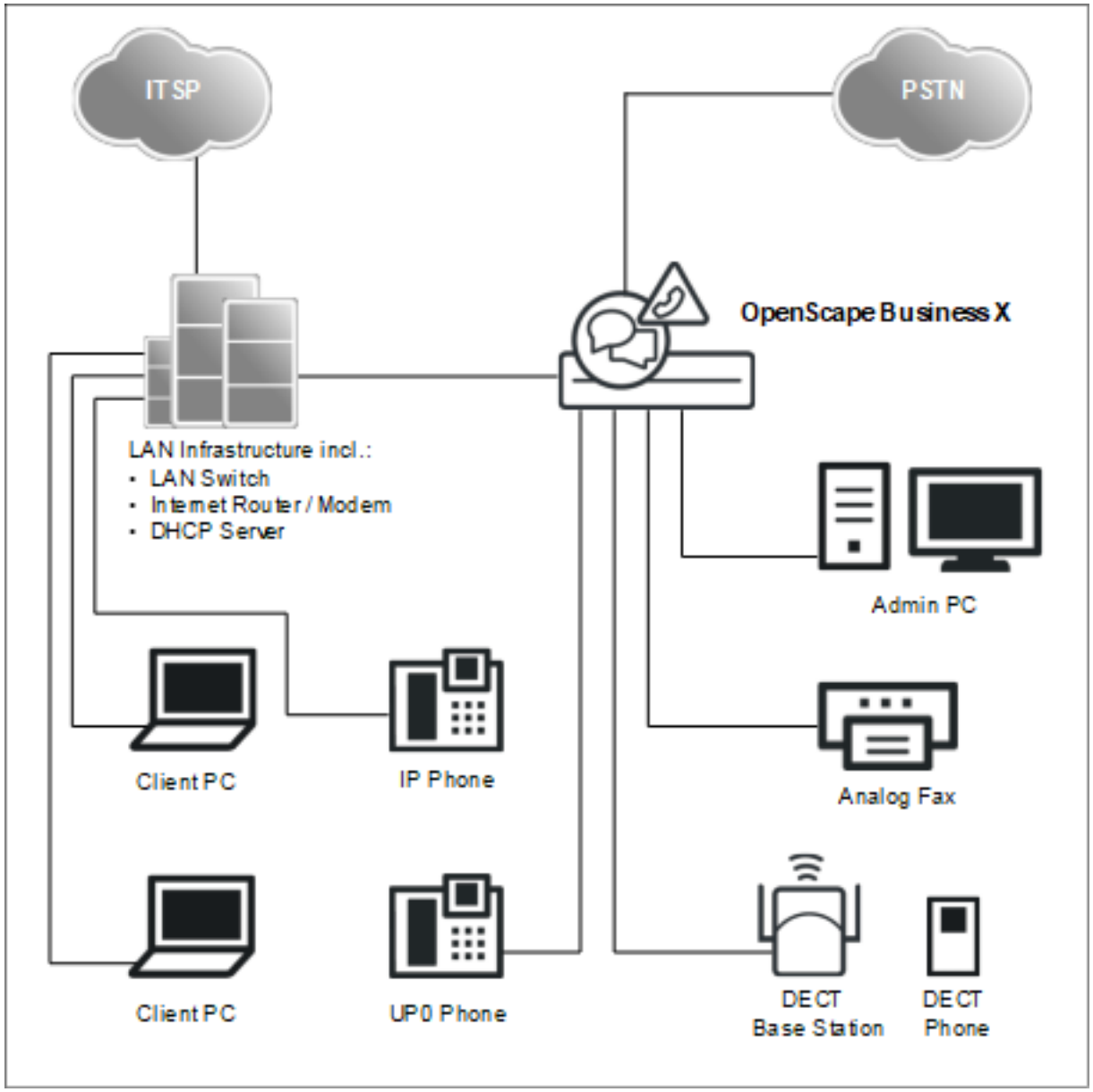
  The IP stations (IP system phones, client PCs, WLAN Access Points, etc.) are integrated in the LAN via one or more switches.
- UP0 stations

  UP0 stations (e.g., OpenStage 60 T TDM system telephones) are connected directly to the communication system.
- Analog stations

  Analog stations (e.g., analog fax devices) are connected directly to the communication system.
- DECT stations

  DECT stations are logged on to the communication system via a base station.

The IP clients receive their IP addresses dynamically from an internal or external DHCP server (e.g., an Internet router).



5.3 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call numbers.

Default Dial Plan

The internal call numbers are preassigned default values. These values can be adapted to suit individual requirements as needed (e.g., to create individual dial plans).

Extract from the default dial plan:

Type of call numbers	**X1**	X3/X5/X8
Internal station numbers	11-30	100-742
User direct inward dialing numbers	11-30	100-742
Trunk station number	700-703	from 7801 onward
Seizure codes (external codes): Trk. Grp 1 (trunk: ISDN, analog) Rte. 8 (UC Suite) Trk. Grp 12-15 (trunk: ITSP) Rte. 16 (Networking)	 0 = World / 9 = USA - not preset not preset	 0 = World / 9 = USA 851 855-858 859
Call number for remote access	not preset	not preset
Call number for voicemail UC Smart UC Suite	351 -	351 not preset

Individual Dial Plan

An individual dial plan can be imported via an XML file during basic configuration.

The XML file contains several tabs. Besides the names and phone numbers of subscribers, the "Customer" tab also includes additional subscriber data such as the subscriber types and e-mail addresses of the subscribers.

A sample XML file with the appropriate explanations can be found in the WBM under **Service Center** > **Documents** > **CSV Templates**. You can also use the XML file stored there as a template for your data. It can be edited with Microsoft Excel, for example.

5.4 IP Address Scheme

An IP address scheme is a definition of how the IP addresses are used in the customer LAN. It includes the IP addresses of PCs, servers, Internet routers, IP phones, the communication system, etc.

To provide a better overview of the assignment of IP addresses, an IP address scheme should be created.

Example of an IP address scheme with the IP address range `192.168.1." -x`:

IP address range	**Clients**
192.168.1.1 to **192.168.1.19**	Clients with a fixed IP address:
192.168.1.1	Internet router (gateway)
192.168.1.2	Communication system
192.168.1.3	Application Board (optional)

IP address range	Clients
192.168.1.10	E-mail server
192.168.1.50 to **192.168.1.254**	Client PCs & IP phones, also the IP address range of the DHCP server; IP addresses are assigned automatically to the clients

The following IP address ranges are internally reserved and must not be used:

Connected IP address ranges	Description
10.0.0.1; 10.0.0.2	Reserved for the license server
10.186.237.65; 10.186.237.66	Reserved for remote ISDN (obsolete)
192.168.3.2	Internal IP address of the communication system
192.168.2.1	IP address of the LAN3 port (Admin port)

This list can also be found in the WBM under **Service Center** > **Diagnostics** > **Status** > **Overview of IP Addresses**.

Expanding the netmask when using the default network segment

Both the internal IP address of the communication system and the IP address of the LAN3 port (Admin port) must not be in the same network segment as the IP address of the communication system.

Default network segment configuration:

- 192.168.1.2: IP address of the communication system
- 255.255.255.0: Netmask
- 192.168.3.2: Internal IP address of the communication system
- 192.168.2.1: IP address of the LAN3 port (Admin port)

If the netmask when using the default network segment of 255.255.255.0 was expanded to 255.255.0.0, for example, then the above IP addresses need to be changed:

Example of a modified configuration:

- 192.168.1.2: IP address of the communication system
- 255.255.**0**.0: Netmask
- 192.**169**.3.2: Internal IP address of the communication system

  The change is made via **Expert mode** > **Telephony** > **Payload** > **HW Modules** > **Edit DSP Settings**
- 192.**170**.2.1: IP address of the LAN3 port (Admin port)

  The change is made via **Expert mode** > **Telephony** > **Network Interfaces** > **Mainboard** > **LAN 3 (Admin)**

5.5 Initial Startup

Initial startup includes starting up the communication system, connecting and configuring the admin PC and starting the OpenScape Business Assistant (WBM) administration program for the first time.

The initial startup of the communication system must be performed prior to integrating the communication system into the internal LAN. Problems can occur if the pre-configured IP address of the communication system already exists in the internal LAN and/or if a DHCP server is already in use. In such cases, the IP address of the communication system must first be reconfigured and/or the DHCP server of the communication system must be deactivated. Only then can the communication system be integrated into the internal LAN.

NOTICE: Prior to initial startup, please follow the instructions on data protection and data security.



DANGER: OpenScape Business X8 may only be powered up if all system boxes are sealed at the rear with the connection and filler panels provided.



DANGER: OpenScape Business X3/X5 must not be powered on unless the housing front is closed. Always use dummy panels (C39165-A7027-B115) to cover slots that are not equipped with boards.



DANGER: The OpenScape Business X1W/X3W/X5W must only be switched on when the housing is closed.

Connecting the admin PC

To configure the communication system, the admin PC is directly connected to the "LAN" interface of the communication system. The communication system is then configured to obtain its IP address from the internal DHCP server of the communication system. After successful installation, the admin PC can be integrated into the internal LAN without any further configuration changes.

5.5.1 How to Restart the Communication System

Prerequisites

The hardware was correctly installed (see *OpenScape Business Installation Guide*).

The memory card (with the system software) was inserted.

The communication system has not been integrated into the customer LAN yet.

Step by Step

Connect the communication system to the power supply.

WARNING:

Risk of electric shock through contact with live wires

Make sure that the communication system (and for OpenScape Business X8, each system box) is grounded by a separate ground wire (see *OpenScape Business Installation Guide*).

The communication system is now started up, During this process, the system LEDs light up in different colors and sequences (see the *OpenScape Business Installation Guide* for details). During startup, the communication system must not be disconnected from the power supply.

After completion of the startup, the "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

5.5.2 How to Connect the Admin PC to the Communication System

Prerequisites

The communication system is ready for use.

Step by Step

1) Start the admin PC.

2) Check whether a dynamic IP address can be assigned to the PC. If not, you will have to reconfigure the admin PC. To do this you must have Administrator rights.

NOTICE: The IP settings described here apply to Windows 7. For more detailed information on the configuration for other Windows operating systems, please refer to the appropriate operating system instructions.

a) Select **Start** > **Control Panel**, double-click on **Network and Internet** and then click **Network and Sharing Center**.

b) Click on **LAN connection** for the appropriate active network and then click **Properties**.

c) On the **Networking** tab, use the left mouse button to select the **Internet Protocol Version 4(TCP/IPv4)** entry and then click on **Properties**.

d) Click on the **General** and ensure that the radio button **Obtain an IP address automatically** is enabled. If it is not, then activate it.

e) Close all open windows with **OK**.

3) Connect the just configured LAN port of the admin PC to the LAN port "LAN" of the communication system using a LAN cable. The admin PC is assigned a dynamic IP address via this interface.

NOTICE: You can also connect the admin PC to the LAN port "Admin" of the communication system, but you will then need to assign a fixed IP address in the range 192.168.2.xxx (e.g., 192.168.2.40) and the network mask 255.255.255.0 to the admin PC. The communication system has the IP

address 192.168.2.1 via the LAN port "Admin" - important for WBM access!

5.5.3 How to Start the WBM

Prerequisites

The communication system is ready for use. The "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

The admin PC and the communication system can communicate with one another over the LAN.

Step by Step

1) Start the web browser on the admin PC and open the login page of the OpenScape Business Assistant (WBM) at the following address:

`https://192.168.1.2`

NOTICE: If the WBM cannot be started, check the LAN connection and repeat the call. If it still cannot be started, check whether the IP address has been blocked by your PC's internal firewall. More detailed information can be found in the documentation of your firewall

2) If the browser reports a problem with a security certificate, install the certificate (using the example of Internet Explorer V10).

a) Close the web browser.
b) Open the web browser with administrator rights by clicking the right mouse button on the web browser icon and selecting the menu item **Run as administrator** from the context menu.
c) Allow the User Account Control.
d) Open the login page of the OpenScape Business Assistant (WBM) at the following address:

`https://192.168.1.2`

e) Click on **Continue to this website**.
f) Click on the message **Certificate Error** in the navigation bar of the web browser.
g) Click on **View Certificates**.
h) Click on **Install Certificate** (only visible with administrator rights).
i) Select the option **Local Computer** and confirm with **Next**.
j) Select the option **Place all certificates in the following store**, click **Browse** and specify **Trusted Root Certification Authorities**.
k) Confirm with **OK** and then with **Next** and **Finish**.
l) Confirm the certificate import with **OK** and close the certificate window **OK**.
m) Close the web browser.
n) Start the web browser again (without administrator rights) and open the login page of the OpenScape Business Assistant (WBM) at the following address:

`https://192.168.1.2`

3) Click on the language code at the top right and select the language in which the user interface of the WBM is to be displayed from the menu. The Login page will be displayed in the selected language.
4) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> **NOTICE:** If you go to the **Password** field after entering `administrator`, `@system` will be added automatically.

5) In the second field under **Login**, enter the default password `administrator` for access as an administrator.
6) Click **Login**.
7) The following steps are only required once when first logging on to the WBM:
   a) Reenter the default password **administrator** in the `Password` field.
   b) Enter a new password in the **New Password** and **Confirm New Password** fields to protect the system against misuse. Note case usage and the status of the `Num` und `CapsLock` keys. The password is displayed as a string of asterisks (*).

> **NOTICE:** The password must be at least 8 characters long and include a digit. Make sure that you remember your new password.

   c) Click **Login**.
   d) Select the current date and enter the correct time.
   e) Click **OK & Next**. You are automatically logged out of the WBM.
   f) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> **NOTICE:** If you go to the **Password** field after entering `administrator`, `@system` will be added automatically.

   g) In the second field under **Login**, enter your new password for access as an administrator.
   h) Click **Login**. The home page of the WBM appears.

Next steps

Start the initial installation.

5.6 Integration into the Customer LAN

The WBM wizard **Initial Installation** is used for integration into the customer LAN. This wizard guides you through the basic settings for integrating the communication system into the existing LAN.

5.6.1 How to Start the Initial Installation Wizard

Prerequisites

The WBM has been started.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Initial Installation** wizard.

> **NOTICE:** If the size of the browser window cannot display the workspace in its entirety at low screen resolutions, a horizontal or vertical scroll bar appears at the sides and can be used to scroll to the required section.

Next steps

Perform initial installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

5.6.2 System Settings

The **System Settings** window is used to configure the system settings of the communication system.

Proceed as follows:

1) Set the display logo and the product name

   Specify a display text to be displayed on the display of the system phones. Additionally, you can also select the product name.
2) Edit IP addresses (if required)

   By default, the communication system is assigned an IP address and a subnet mask. You may need to adjust the IP address and/or subnet mask to your own IP address range.

   In addition, you can specify the IP address of your default router, e.g., the IP address of the Internet router.

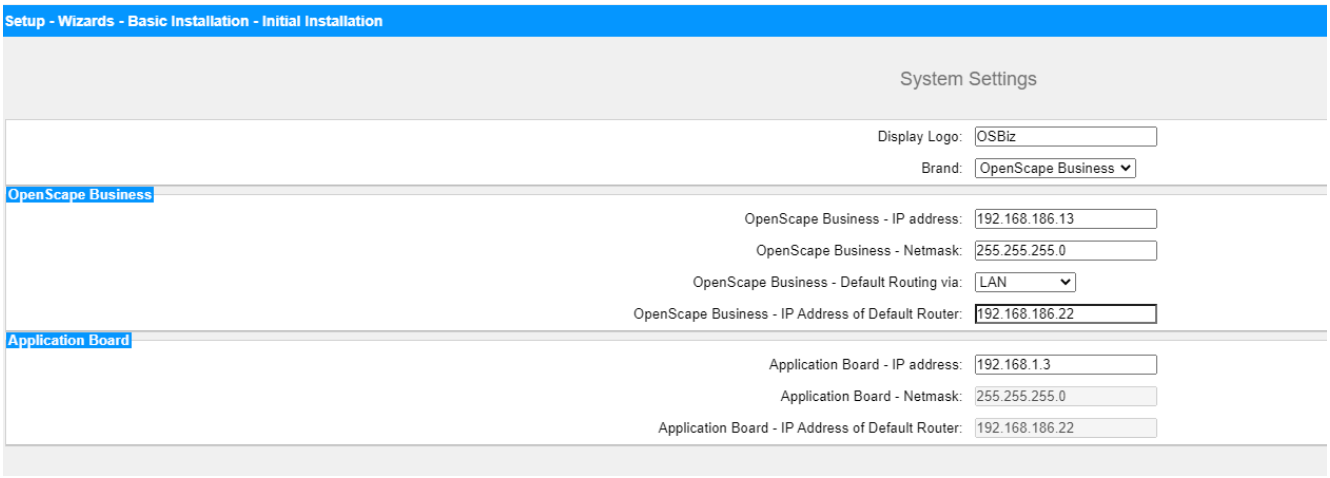
   The Application Board (UC Booster Card) also requires an IP address. You can assign an IP address from your IP address range regardless of whether or not the board is installed.

If the netmask is to be expanded, e.g., from 255.255.**255**.0 to 255.255.**0**.0, both the internal IP address of the communication system and the IP address of the LAN3 port (Admin port) must be changed because they are not allowed to be in the same network segment as the IP address of the communication system (see also IP Address Scheme).

5.6.2.1 How to Set the Display Logo and the Product Name

Prerequisites

You are in the **System Settings** window.



Step by Step

1) In the **Display Logo** field, enter a text of your choice (e.g., OpenScape Biz). The text can contain up to 16 characters. Avoid the use of diacritical characters such as umlauts and special characters.
2) Select the desired time product name in the **Brand** drop-down list.

Next steps

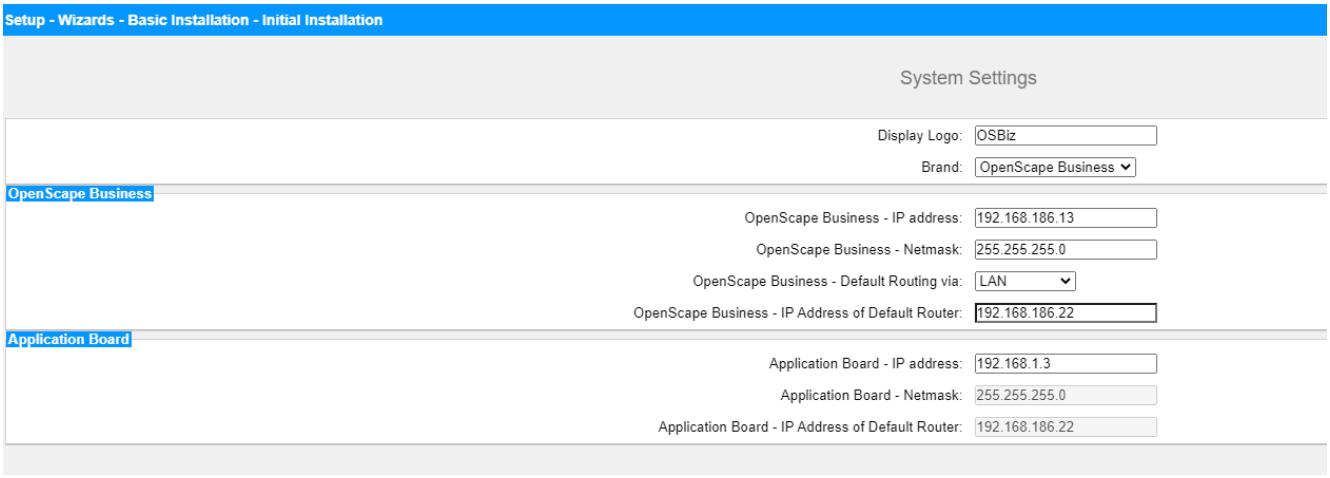
Edit IP addresses (if required) or configure DHCP.

5.6.2.2 How to Specify the IP Addresses (Optional)

Prerequisites

You know the IP address range of your internal network.

You are in the **System Settings** window.



Step by Step

1) Specify the IP address of the communication system:
   a) In the field **OpenScape Business - IP address**, enter an IP address that lies within the IP address range of your internal network (e.g., internal network: `192.168.1.x`, OpenScape Business: `192.168.1.2`.

      NOTICE: The IP address for OpenScape Business must not be assigned to any other existing network client, since this would result in an IP address conflict.

   b) Enter the subnet mask of your internal network (e.g., `255.255.255.0`) in the **OpenScape Business - Subnet Mask** field.
2) Specify the IP address of the default router:
   a) In the **OpenScape Business - Default Routing via** field, select the entry **LAN**.
   b) Enter the IP address of your default router in the **OpenScape Business - IP Address of Default Router** field (e.g., internal network: `192.168.1.x`, Internet router as default router: `192.168.1.1`).
3) Specify the IP address of the UC Booster Card (required if installed):
4) Click on **OK & Next**.

Next steps

Configure DHCP.

5.6.2.3 How to Specify the Device Name

Prerequisites

You are in the **System Settings** window.

System is in DTAG mode.

Step by Step

1) Check the **Automatic RSP.servicelink registration** checkbox:

   Device Name field is editable.
2) Specify the **Device Name**.

   By selecting the Automatic RSP.servicelink registration, system will try automatically every 10 minutes to register and connect to RSP servers using the provided Device Name.
3) Click on **OK & Next.**

Next steps

Configure DHCP.

5.6.3 DHCP Settings

In the window **DHCP global settings** enable and configure or disable the internal DHCP server of the communication system.

A DHCP server automatically assigns a unique IP address to each IP station (IP system phones, PCs, etc.) and provides the IP stations with network-specific data such as the IP address of the default gateway (Internet router), for example.

The DHCP server can be an external DHCP server (e.g., the DHCP server of the Internet router) or the internal DHCP Server of the Linux server integrated into the communication system.

Either the integrated DLI of the communication system or an external DLS server can be used for automatically updating the software of the IP system phones (Deployment Service (DLS and DLI)). The IP address of the integrated DLI or the external DLS server must be known to the DHCP server.

You have the following options:

- Enable and configure the internal DHCP server

  If the internal DHCP server of the communication system is used, an external DHCP server (e.g., the DHCP server of the Internet router) must be deactivated. The settings of the internal DHCP server may have to be adapted to the customer LAN. If the internal DHCP server and the internal DLI are used, the system phones are updated automatically. If an external DLS server is used, its IP address must be entered in the internal DHCP server using Expert mode (Deployment Service (DLS and DLI)).
- Disable the internal DHCP server

  If an external DHCP server is used, the internal DHCP server of the communication system must be disabled. For IP system phones to be automatically supplied with the latest phone software, network-specific data (such as the IP address of the internal DLI or the external DLS server) must be specified on the external DHCP server.

NOTICE: Not all external DHCP servers support the entry of network-specific data! In this case, the data must be entered manually on all IP system phones.

5.6.3.1 How to Disable the Internal DHCP Server

Prerequisites

An external DHCP server (e.g., the DHCP server of the Internet router) is enabled in the internal network.

You are in the **DHCP Global Settings** window.

Step by Step

1) Clear the **Enable DHCP Server** check box.
2) Click on **OK & Next**.

Next steps

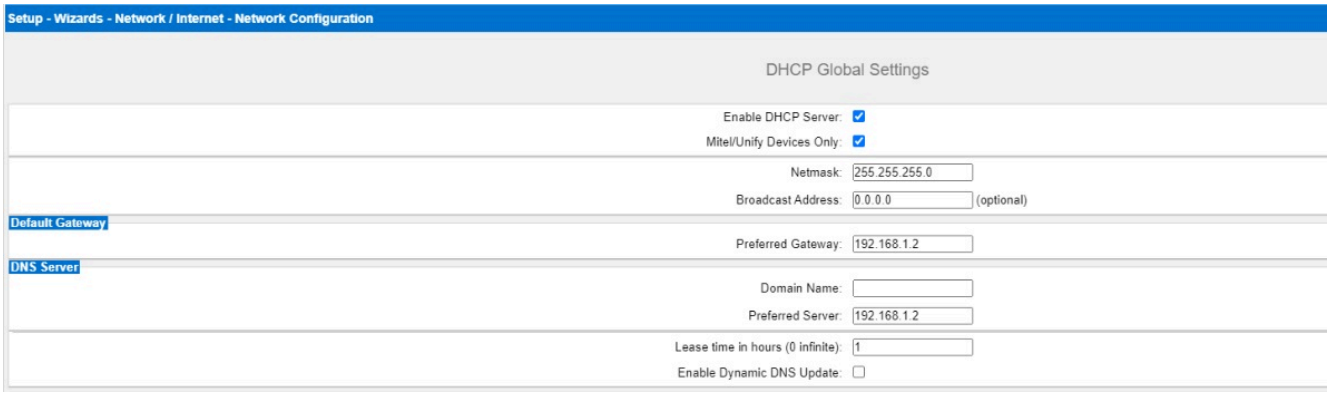
Configure country and time settings.

5.6.3.2 How to Enable and Configure the Internal DHCP Server

Prerequisites

The external DHCP server (e.g., the DHCP server of the Internet router) has been disabled in the internal network.

You are in the **DHCP Global Settings** window.



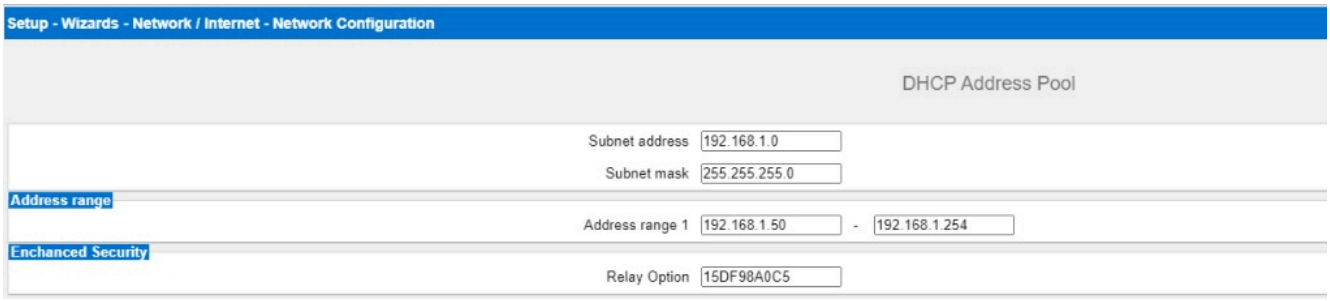
Step by Step

1) Leave the **Enable DHCP Server** check box enabled.
2) If needed, enable the **Mitel/Unify Devices Only** checkbox.

NOTICE: This option is only available for V3 mainboards.

---

3) Go to the **Netmask** field and adjust the subnet mask to your IP address range (for example, `255.255.255.0`).
4) In the field **Preferred Gateway**, enter the IP address of the Internet router (e.g., `192.168.1.1`).
5) In the field **Preferred Server**, enter the IP address of the DNS server (e.g., the IP address of the Internet router, `192.168.1.1`.
6) Click on **OK & Next**. The **DHCP Address Pool** window appears.



7) Specify the values for **Subnet address**, **Netmask** and **Address range 1** in order to define the IP address range to be managed by the internal DHCP server.

   If the internal network uses static IP addresses (e.g., for a printer server), the IP address range (DHCP address pool) must be selected so that the fixed IP addresses are not included within this range.

   Example:

   Internet router: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnet address: `192.168.1.0`

   Subnet mask: `255.255.255.0`

   Printer Server: `192.168.1.10`

   DHCP address pool: `192.168.1.50` to `192.168.1.254`

8) If needed, specify the value of the **Relay Option** field.

   NOTICE: This option is only available for V3 mainboards.

9) Click on **OK & Next**.

Next steps

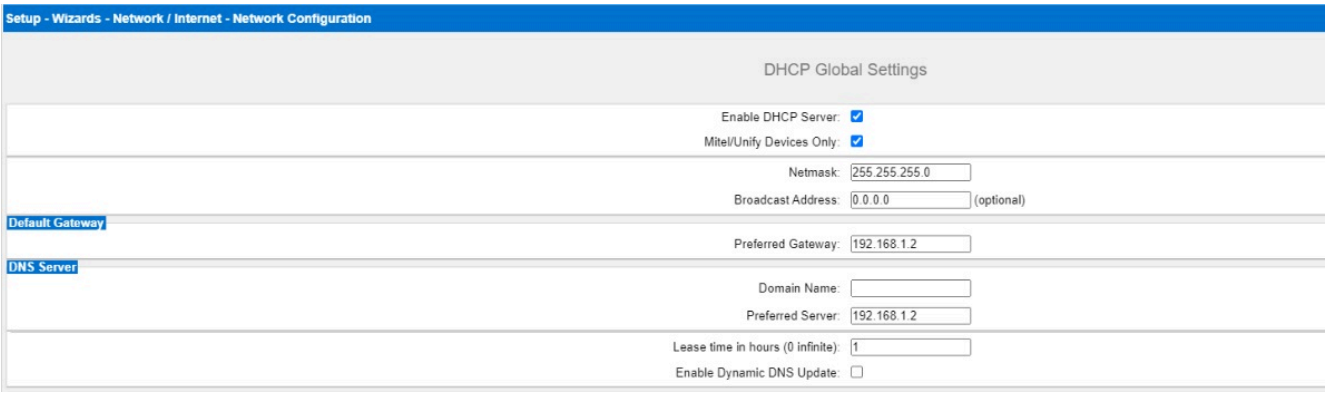
Configure country and time settings.

5.6.3.3 How to Enable DHCP for Mitel/Unify Devices Only

This option allows the system administrator to activate the OpenScape Business DHCP service exclusively for Mitel and Unify devices.

Prerequisites

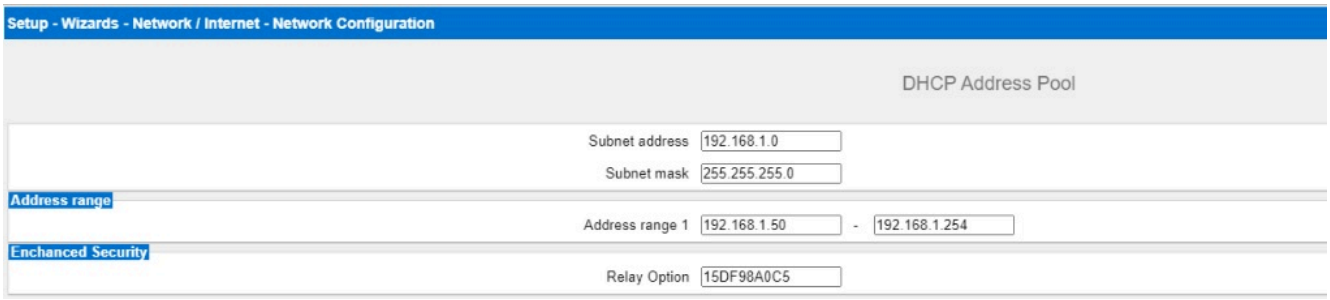
You are in the **DHCP Global Settings** window.



Step by Step

1) Leave the **Enable DHCP Server** check box enabled.

2) Click to enable the **Mitel/Unify Devices Only** checkbox. See DHCP Server > Global Parameters for further information on this option.
3) Go to the **Netmask** field and adjust the subnet mask to your IP address range (for example, `255.255.255.0`).
4) In the field **Preferred Gateway**, enter the IP address of the Internet router (e.g., `192.168.1.1`).
5) In the field **Preferred Server**, enter the IP address of the DNS server (e.g., the IP address of the Internet router, `192.168.1.1`.
6) Click on **OK & Next**. The **DHCP Address Pool** window appears.



7) Specify the values for **Subnet address**, **Subnet mask** and **Address range 1** to define the IP address range to be managed by the internal DHCP server.

   If the internal network uses static IP addresses (e.g., for a printer server), the IP address range (DHCP address pool) must be selected so that the fixed IP addresses are not included within this range.

   Example:

   Internet router: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnet address: `192.168.1.0`

   Subnet mask: `255.255.255.0`

   Printer Server: `192.168.1.10`

   DHCP address pool: `192.168.1.50` to `192.168.1.254`
8) Specify the value of the **Relay Option** field.
9) Click on **OK & Next**.

Next steps

Configure country and time settings.

5.6.4 Country and Time Settings

In the **Basic Configuration** window, select your country and the language for the event logs and set the date and time. If you are using the integrated Cordless solution, enter the system-wide DECT system ID here.

Proceed as follows:

1) Select the country code and the language to be used for event logs

   For country initialization to work correctly, you must select the country in which the communication system is operated. In addition, you can select the language in which the event logs (system event logs, errors logs, etc.) are to be stored.
2) Enter the DECT system identification (only for integrated Cordless solution)

   If you are using the integrated Cordless solution, enter the system-wide DECT system ID here.
3) Setting Date and Time
   - How to Set the Date and Time Manually

     The communication system and the stations (IP phones, TDM phones, client PCs) should have a uniform time base (date and time). If no SNTP server has been specified for time synchronization, the date and time can also be entered manually.

     NOTICE: The date and time are also updated when a connection is set up via an ISDN trunk.
   - How to Obtain the Date and Time from an SNTP Server

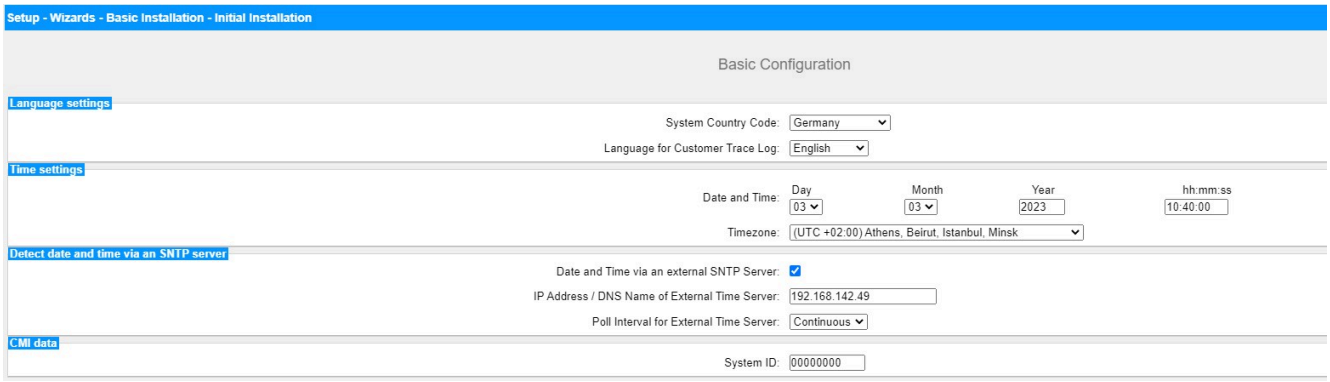
     The communication system and IP stations (IP phones, client PCs) should have a uniform time base (date and time). This time base can be provided by an SNTP server. The SNTP server can be located on the internal network or the Internet.

The IP phones receive the date and time automatically from the communication system. The client PCs on which the UC clients run must be set so that they are synchronized with the communication system (see the operating system instructions for the client PCs).

5.6.4.1 How to Select the Country Code and the Language for Event Logs

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

1) In the **System Country Code** drop-down list, select the country where the communication system is operated.

2) In the **Language for Customer Event Log** field, enter the language in which the event logs (system event logs, error logs, etc.) are to be output.

Next steps

Enter the DECT system identification (only for integrated Cordless solution)

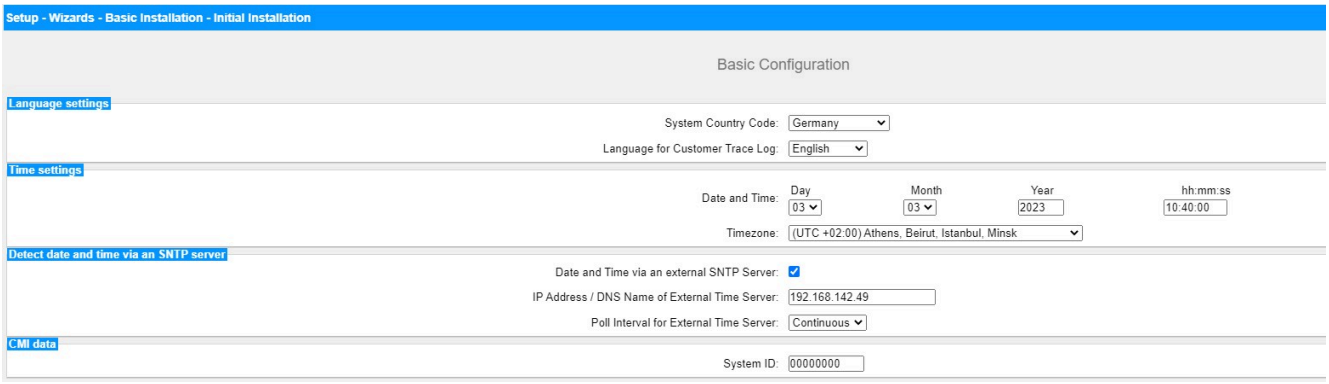
or

Set the date and time manually or obtain the date and time from an SNTP server.

5.6.4.2 How to Enter the DECT System ID

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

In the **CMI data** area under **System ID**, enter the 8-digit hexadecimal DECT system ID that you received on purchasing your integrated Cordless solution.

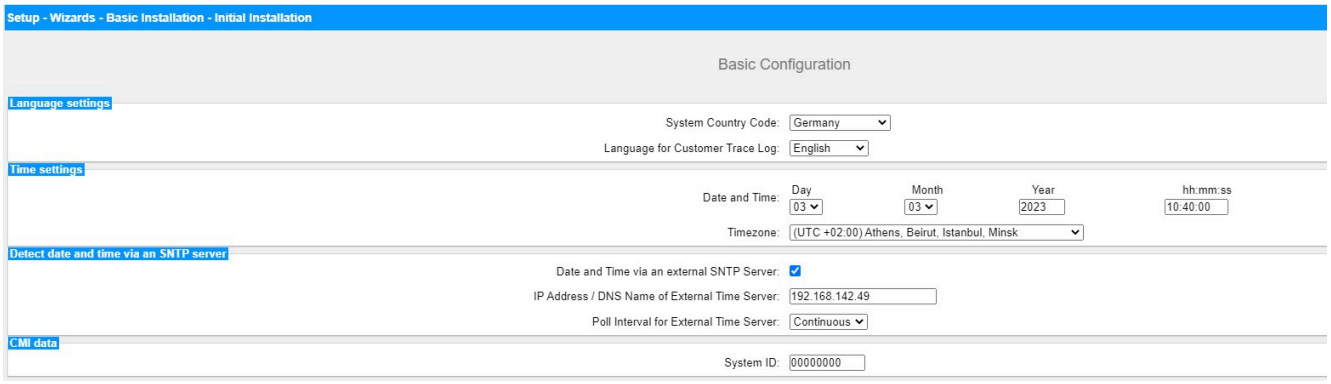
Next steps

Set the date and time manually or obtain the date and time from an SNTP server.

5.6.4.3 How to Set the Date and Time Manually

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

1) Enter the current values for **Date and Time**.
2) Select the desired time zone in the **Timezone** field.
3) Click on **OK & Next**.

NOTICE: In case the Timezone setting is changed, then at the last step of Initial Wizard **the system will be restarted**.

If Timezone setting remain untouched then system will not be restarted.

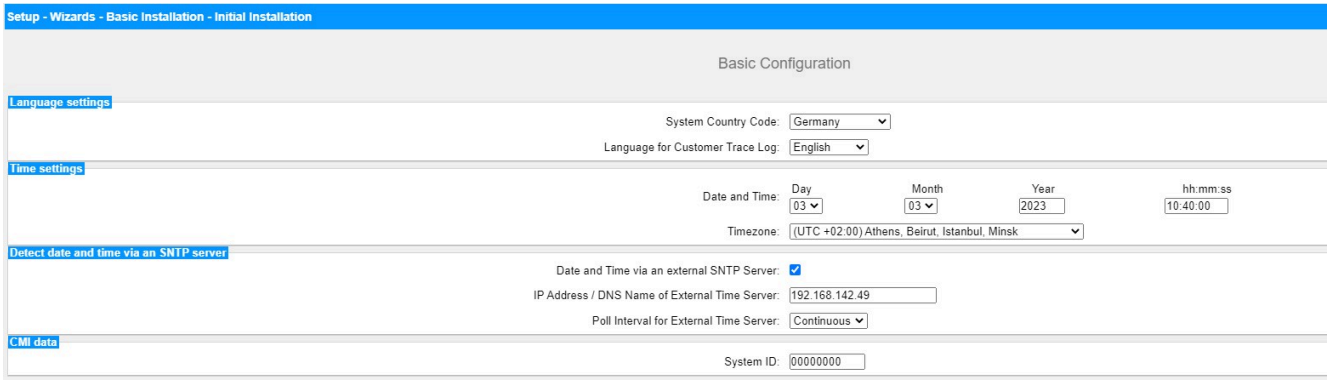
Next steps

Specify UC solution.

5.6.4.4 How to Obtain the Date and Time from an SNTP Server

Prerequisites

You are in the **Basic Configuration** window.



Step by Step

1) Select the **Date and Time via an external SNTP Server** check box.
2) Enter the IP address or the DNS name of the SNTP server (e.g., `0.de.pool.ntp.org`) in the **IP Address / DNS Name of External Time Server** field).

3) From the drop-down list **Poll Interval for External Time Server**, select after how many hours the Date and Time should be synchronized by the SNTP Server (recommended value: `4 h`).
4) Click on **OK & Next**.

Next steps

Specify UC solution.

5.6.5 UC Solution

In the **Change application selection** window, select the UC solution to be used.

You have the following options:

- **Package with UC Smart**

  The UC solution UC Smart is integrated on the OpenScape Business X mainboard.
- **Package with UC Suite**

  The UC solution UC Suite is integrated on the additional internally pluggable "UC Booster Card".
- **Package with UC Suite on OSBiz UC Booster Server**

  The UC solution UC Smart is integrated on the external Linux server "OpenScape Business UC Booster Server".
- **Package with UC Suite on OSBiz UC Booster Server**

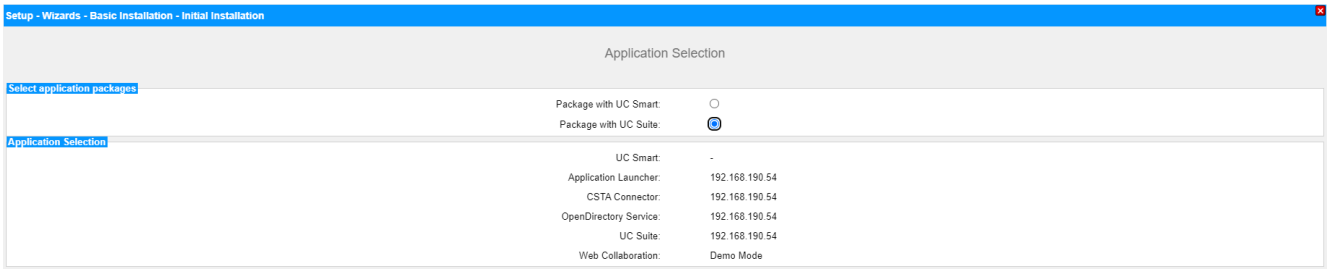
  The UC solution UC Suite is integrated on the external Linux server "OpenScape Business UC Booster Server".

5.6.5.1 How to Define the UC Solution

Prerequisites

You have purchased licenses for either of the UC solutions, UC Smart or UC Suite.

You are in the **Application Selection** window.



Step by Step

1) If you are using the UC solution UC Smart without a UC Booster Server, click **Package with UC Smart**.

2) If you are using the UC solution UC Smart with the UC Booster Server, click on **Package with UC Smart on OSBiz UC Booster Server**. In addition, enter the IP address of the external Linux server "OpenScape Business UC Booster Server" in the **IP address of OSBiz UC Booster Server** field.
3) If you want to use the UC solution UC Suite with the UC Booster Card, click on **Package with UC Suite**.
4) If you are using the UC solution UC Suite with the UC Booster Server, click on **Package with UC Suite on OSBiz UC Booster Server**. In addition, enter the IP address of the external Linux server "OpenScape Business UC Booster Server" in the **IP address of OSBiz UC Booster Server** field.
5) Click on **OK & Next**.
6) The **Initial installation** wizard is closed. Click **Finish**.
7) Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

NOTICE: If IP addresses or DHCP server settings have been changed, the communication system performs a restart. This can take a few minutes.

Next steps

Connect the communication system to the customer LAN.

5.6.6 Connecting the Communication System to the Customer LAN

After a successful initial installation, the communication system is connected to the existing customer LAN.

5.6.6.1 How to Connect the Communication System to the Customer LAN

Prerequisites

The communication system is ready for use.

Step by Step

1) Remove the LAN cable of the admin PC from the central LAN port "LAN" and integrate the admin PC in the customer's LAN by connecting it to a switch, for example.
2) Connect a LAN cable to the middle "LAN" port of the communication system.
3) Integrate the communication system via this LAN cable in the customer LAN by connecting it to a switch, for example.
4) If a UC Booster Card (Application Board) is plugged in, connect another LAN cable to the "LAN2" port of the UC Booster Card (right/lower of the two LAN interfaces) and integrate the UC Booster Card via this LAN cable in the customer LAN by connecting it to a switch, for example.

Next steps

Start the basic configuration.

5.7 Basic Configuration

The **Basic Installation** wizard is used for basic configuration. Basic configuration includes the most important settings for operating the communication system.

The Basic Installation Wizard includes a progress indicator showing the current step, as well as the steps that follow.

5.7.1 How to Start the Basic Installation Wizard

Prerequisites

The **Initial installation** has been completed.

The communication system is integrated in the customer LAN

The communication system is ready for use. The "Run" LED on the mainboard flashes green at 1Hz (0.5 sec on / 0.5 sec off).

Step by Step

1) Open the WBM login page on the admin PC by entering the following address in your web browser:
   `https://<IP address of OpenScape Business>`
   The default IP address for OpenScape Business is `192.168.1.2`, i.e., `https://192.168.1.2`, for example.
2) In the **User Name** field, enter the default user name `administrator@system` for access as an administrator.
3) Enter the password you defined at initial startup in the **Password** field.
4) Click on **Login**.
5) In the navigation bar, click on **Setup**.
6) Click on **Edit** to start the **Basic Installation** wizard.

Next steps

Perform basic installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

5.7.2 System Phone Numbers and Networking

Enter the system phone numbers (PABX number, country and area code, international prefix) in the **Overview** window and specify whether OpenScape Business is to be networked with other OpenScape Business systems.

Proceed as follows:

1) Enter system phone numbers
   - Enter system phone numbers for point-to-point connection

     Here you enter the system phone number for your point-to-point connection and the country code and area code.

     The entry of the country code is mandatory for Internet telephony and conference server functionality.

     The international prefix is preset, depending on the previously dialed country code.
   - Enter system phone numbers for point-to-multipoint connection

     Here you enter the country code and area code for your point-to-multipoint connection.

     The entry of the country code is mandatory for Internet telephony and Meet-Me conferences.

     The international prefix is preset, depending on the previously dialed country code.
2) Activate or deactivate networking

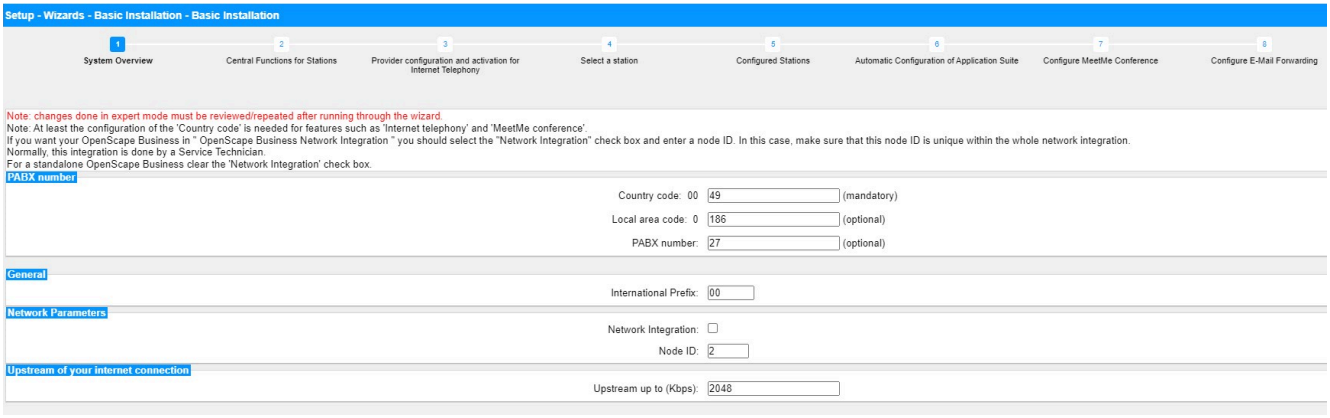
   If OpenScape Business is to be networked with other OpenScape Business systems, networking must be enabled, and OpenScape Business must be assigned a node ID. Every OpenScape Business must have a unique node ID in the network.

5.7.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection

Prerequisites

You have a point-to-point connection.

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.
3) Enter the system phone number of your trunk connection, e.g., `7007` (your connection number), in the **PABX number** field.

4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

Next steps

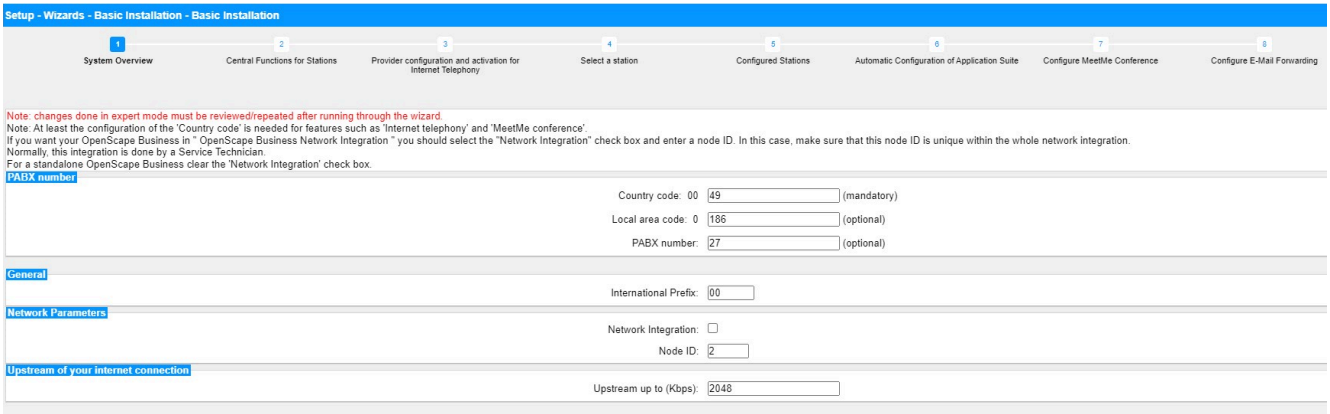
Activate or deactivate networking

5.7.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection

Prerequisites

You have a point-to-multipoint connection.

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.
3) Leave the **PABX number** field empty.
4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

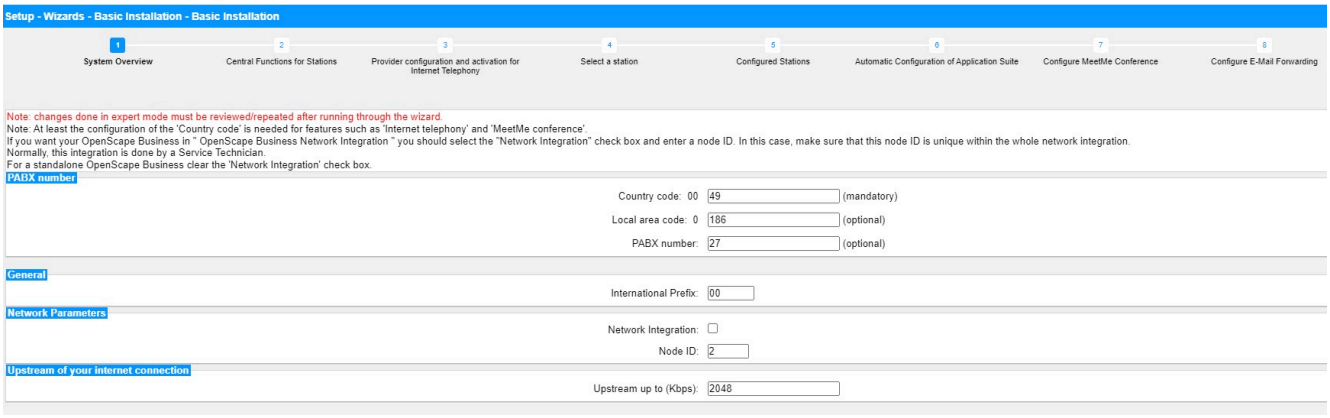
Next steps

Activate or deactivate networking

5.7.2.3 How to Activate or Deactivate Networking

Prerequisites

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) If the communication system is to be networked with other communication systems:
   a) Select the **Network Integration** check box.
   b) In the **Node ID** field for the communication system, enter a node ID that is unique in the internetwork (digits from `1` through `100` are possible).
2) If the communication system is not to be networked with other communication systems, leave the **Network Integration** check box disabled.

Next steps

Configure the upstream of your Internet connection.

5.7.3 Station Data

If necessary, you can configure your own individual dial plan instead of the predefined default dial plan in the **Central Functions for Stations** window and import additional station data. In an internetwork, the default dial plan must be adapted to the dial plan of the internetwork.

The default dial plan contains predefined numbers for different types of stations (IP phones, analog phones, ...) and for special functions (Internet telephony, voicemail box, AutoAttendant, ...).

The station data includes the internal call numbers, DID numbers and names of the stations. This data and other station data can be imported into the communication system during the basic configuration via an XML file in UTF-8 format.

NOTICE: An XML template with the appropriate explanations can be found in the WBM under **Service Center** > **Documents** > **CSV Templates**. You can enter your data in this template by using Microsoft Excel, for example.

You have the following options:

- **Configure station data without an internetwork**

  Proceed as follows:

  1) Display the station data

  You can have all preconfigured station numbers and station data displayed.

  2) Delete all station numbers (optional)

  If you use an individual dial plan, you must delete all preconfigured station numbers.

  3) Adapt preconfigured station numbers for the individual dial plan (optional)

  If you are using an individual dial plan, you can adapt the preconfigured phone numbers to your own dial plan.

  NOTICE: If the user passes through the **Change preconfigured functional call numbers,** any existing custom configuration done in UC Suite must be reviewed or repeated (e.g., pilot queues)

  4) Import station data from an XML file (optional)

  You can easily import your individual station numbers, including any additional station data, during the basic configuration via an XML file.

- **Configure station data with an internetwork**

  Proceed as follows:

  1) Delete all station numbers

  If the UC Suite is used in an internetwork, a closed numbering plan is required, i.e., all station numbers in the internetwork must be unique. For this reason, any preconfigured station numbers must be deleted and only stations numbers adapted for the internetwork must be used.

  2) Import station data from an XML file

  The station numbers adapted for the internetwork and any additional station data can be easily imported during the basic configuration via an XML file. This file can contain all stations in the internetwork. During import, only the station numbers and the station data assigned to the previously specified node ID of the communication system will be transferred.

Related tasks

How to display Mass data on page 156
How to Reset the LCR Entries on page 1345

Related reference

LCR > LCR flags on page 1533

5.7.3.1 How to Display the Station Data

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Select the **Display stations configuration** radio button.
2) Click on **Execute function**. A list of stations with the preconfigured phone numbers (default dial plan) is displayed.
3) Click on **OK**. You are taken back to the **Central Functions for Stations** window.
4) If you do not want to change any station data, click **OK & Next**.

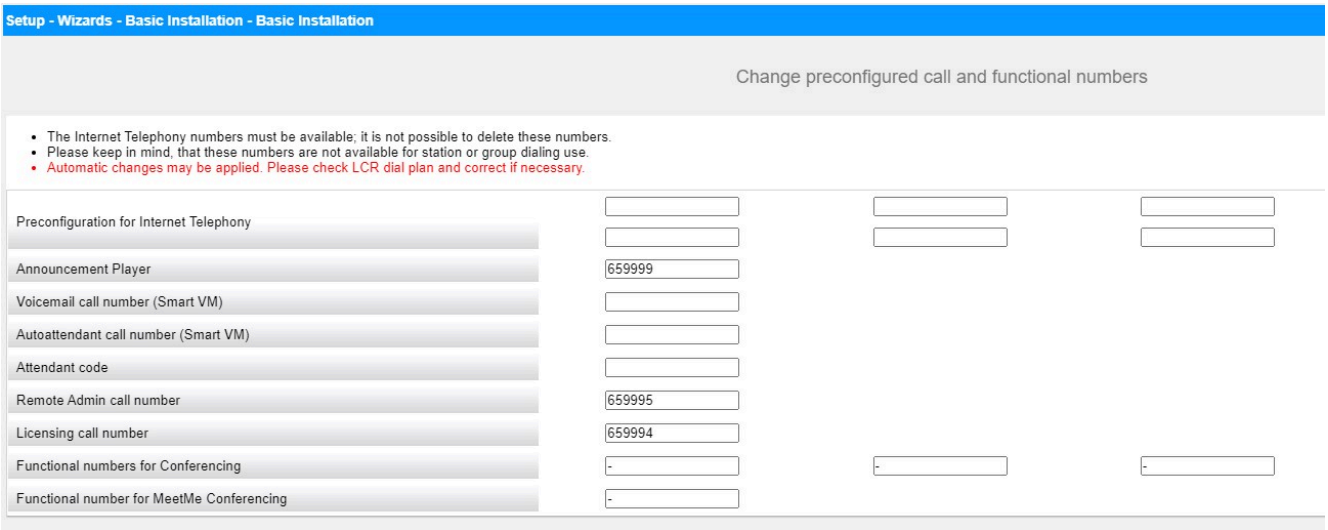
5.7.3.2 How to Delete all Call Numbers

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Enable the radio button **Delete all station call numbers**.
2) Enable the check box **Delete All Call Addresses**.
3) Click on **Execute function**. All preset call numbers are deleted except **Announcement Player, Remote Admin call number** and **Licensing call number**. The **Change preconfigured call and functional numbers** window then appears.



4) Adjust the codes and special call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.
5) If you do not want to change any further station data, click **OK & Next**.

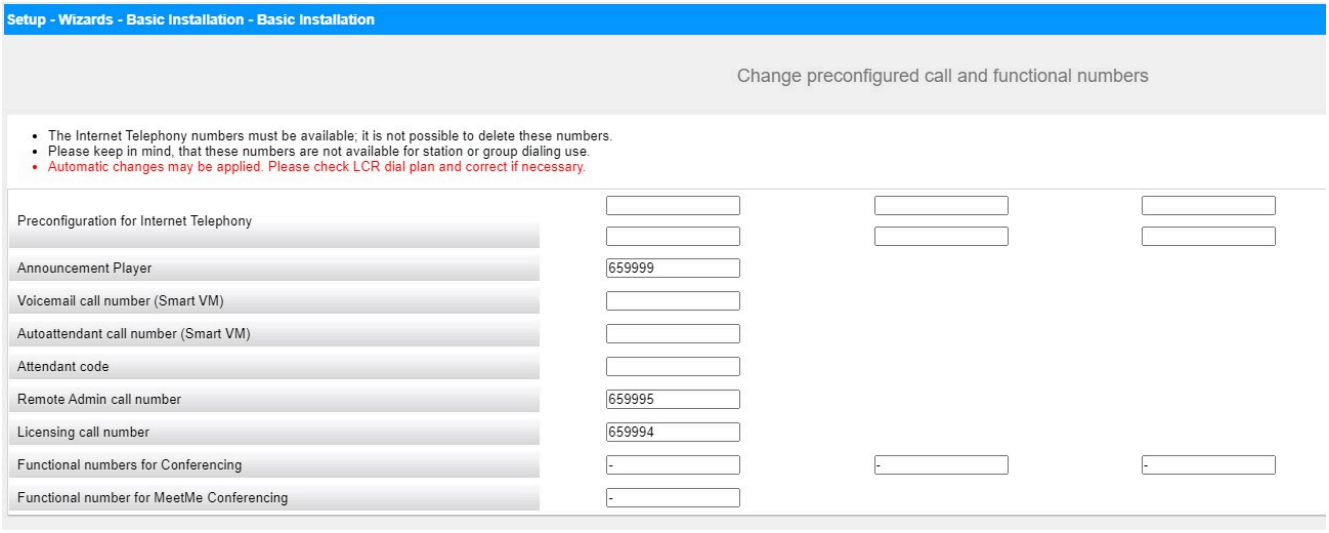
5.7.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Enable the radio button **Change preconfigured call and functional numbers**.
2) Click on **Execute function**. The **Change preconfigured call and functional numbers** window appears.



3) Adjust the preconfigured call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.
4) If you do not want to change any further station data, click **OK & Next**.

5.7.3.4 How to Import the Station Data from an XML File

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

An XML file with the entered data is available in UTF-8 format. An XML template can be found under **Service Center** > **Documents** > **CSV Templates**.

Step by Step

1) Enable the radio button **Import CSV/XML file with station data**.
2) Click **Execute function**.
3) Use **Browse** to select the created XML file and click **Open**.
4) Click **OK** when finished. The station data is imported.
5) Click **OK & Next**.

5.7.3.5 How to display Mass data

Prerequisites

- You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.
- You can also have access to **Mass Data** wizard from **Setup** > **Wizards**.

Step by Step

1) Enable the **Mass Data wizard** button.
2) Click on **Execute function**.
3) In the **Mass Data Wizard** window you can validate the entries of the system, by clicking on **Validate**. There are two types of validation, the Front End Consistency Check and the Back End Consistency Check.
   The green color in validation field indicates only the actions that have been recently validated. The validation of data is not saved, so if the values are changed the user has to validate again the data.
4) During Back End Consistency Check and after the successful validation of data no editing in **Mass Data Wizard** window is possible. After the successful validation **OK&Next** becomes available with Edit restrict mode. If the user clicks on **Back**, Edit mode becomes available but **OK&Next** disappears. When the validation is unsuccessful Edit mode remains intact and **OK&Next** stays hidden.

   NOTICE: The user can click on **Back** to re-edit the data and the window returns to Edit mode again. The Edit restrict mode ensures that the user cannot click on OK&Next and submit changes that are not validated.

5) When **Mass Data Wizard** is configured successfully click on **Finish**. In the finish page is displayed a sum up with all the changes.

   Fields that are not editable are already filled in with the relevant values obtained by the Database. As a result Copy/paste function will have no effect in data.

   Type field is a selectable drop down menu with editing functionality. However the only options accepted are No Port, System Client, SIP Client, Deskshare User and potentially a predefined value based on the Board it belongs. If the user tries to enter something else then this will not be accepted and drop down menu will not be disappear persisting in providing a proper entry.

   Another restriction is that some ports are not changeable (for instance ports belonging in an Analog card, type is not changeable and should remain Analog Station).All restrictions apply when the user tries to perform copy paste on top of Type column. If the user tries to paste irrelevant data not compromising with the rules above paste will not be performed at all.

   Copy and paste can be applied on the whole table as well as on specific parts.

   NOTICE: When selecting two following cells, with a numeric value, and you pull down the fields the following columns are not filled in with ascending numbers but they are filled in with a copy of the selected cells.

Related concepts

Station Data on page 153

5.7.4 ISDN Configuration

In the **ISDN Configuration** window, you specify whether ISDN stations are to be connected and whether ISDN is to be used for the trunk connection. The ISDN trunk connection can be set up as an ISDN point-to-point connection and/or an ISDN-point-to-multipoint connection. Depending on the communication system and board used, different S_0 ports are available for this purpose.

You have the following options:

- Enable ISDN configuration:
  1) Configure an ISDN point-to-point connection

     You can set up an ISDN trunk connection as a point-to-point connection with DID numbers.
  2) Configure an ISDN point-to-multipoint connection

     You can set up an ISDN trunk connection as a point-to-multipoint connection with MSN.
  3) Set up a connection for ISDN subscribers (optional)

     One or more S_0 interfaces can be configured as internal S_0 connections in order to connect ISDN stations (ISDN phones or ISDN fax devices). A station license is required for each ISDN station.
- Disable ISDN configuration

  If you do not have an ISDN trunk connection, you must disable the ISDN configuration. All S_0 interfaces automatically configured as internal S_0ports.

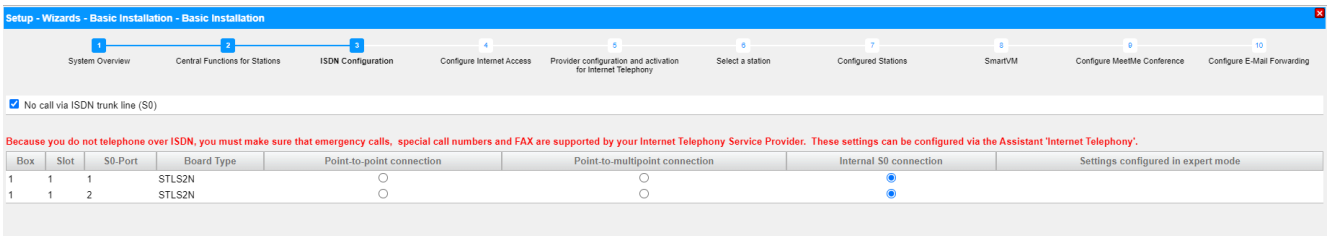
Other options for trunk connections

Instead of setting up an ISDN trunk connection, you can also set up an analog trunk connection or a trunk connection through an Internet Telephony Service Provider (ITSP, SIP provider). Basic installation must be complete before the analog trunk connection can be configured.

5.7.4.1 How to Configure the Connection of ISDN Stations

Prerequisites

You are in the **ISDN Configuration** window of the **Basic Installation** wizard.



Step by Step

1) Clear the check box **No call via ISDN trunk line (S0)**.
2) Activate the **Internal S0 connection** radio button for the desired S_0 port.

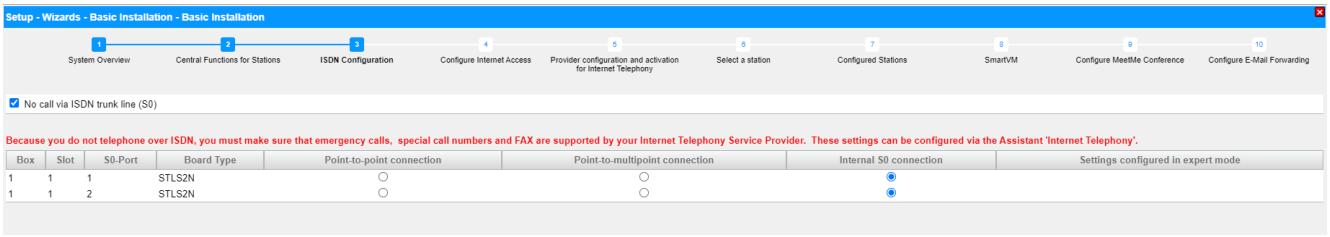
Next steps

Configure ISDN point-to-point connection and/or configure ISDN point-to-multipoint connection.

5.7.4.2 How to Configure the ISDN Point-to-Point Connection

Prerequisites

You are in the **ISDN Configuration** window of the **Basic Installation** wizard.



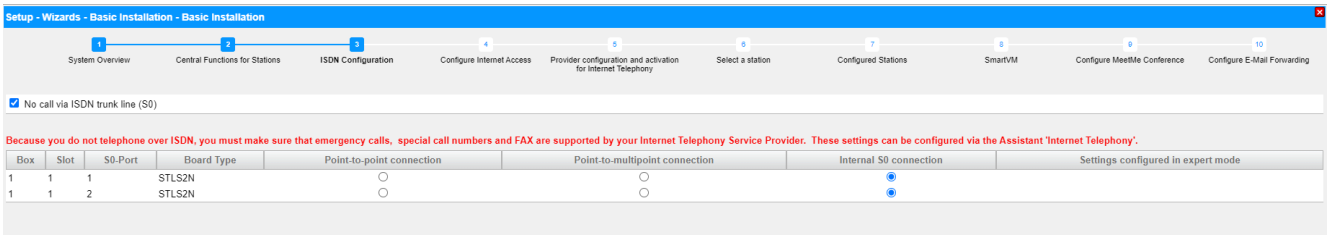
Step by Step

1) To configure the ISDN trunk connection, clear the check box **No call via ISDN trunk line (S0)**.
2) Enable the radio button **Point-to-point connection** for the desired S_0 port.
3) Click on **OK & Next**.

5.7.4.3 How to Configure the ISDN Point-to-Multipoint Connection

Prerequisites

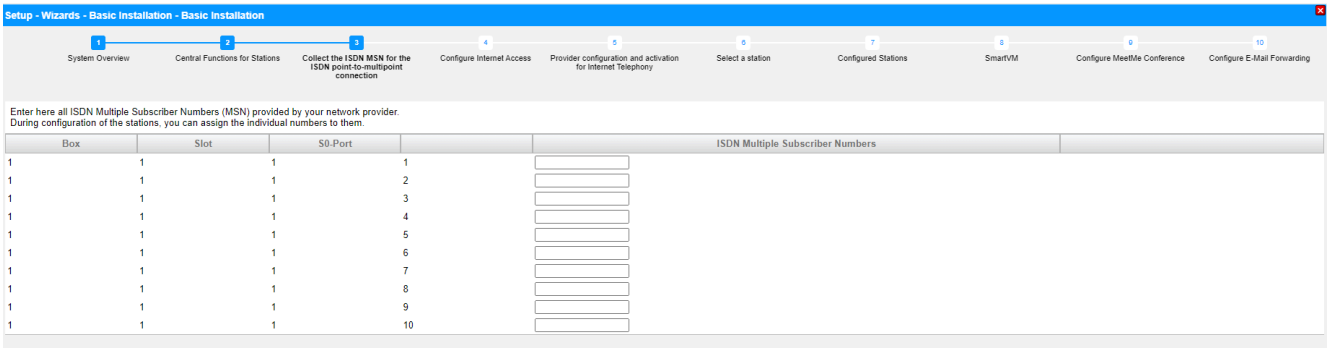
You are in the **ISDN Configuration** window of the **Basic Installation** wizard.



Step by Step

1) To configure the ISDN trunk connection, clear the check box **No call via ISDN trunk line (S0)**.
2) Enable the radio button **Point-to-multipoint connection** for the desired S**0** port.

3) Click on **OK & Next**.



4) Enter all phone numbers (MSNs) supplied by your provider in the **ISDN multiple subscriber numbers** column. You can enter up to 10 MSNs for each S_0 port. The number of the S_0 connections depends on the communication system and possibly the board being used.
5) Click on **OK & Next**.

5.7.4.4 How to Deactivate the ISDN Configuration

Prerequisites

You are in the **ISDN Configuration** window of the **Basic Installation** wizard.

Step by Step

1) Select the **No call via ISDN trunk line (S0)** check box.

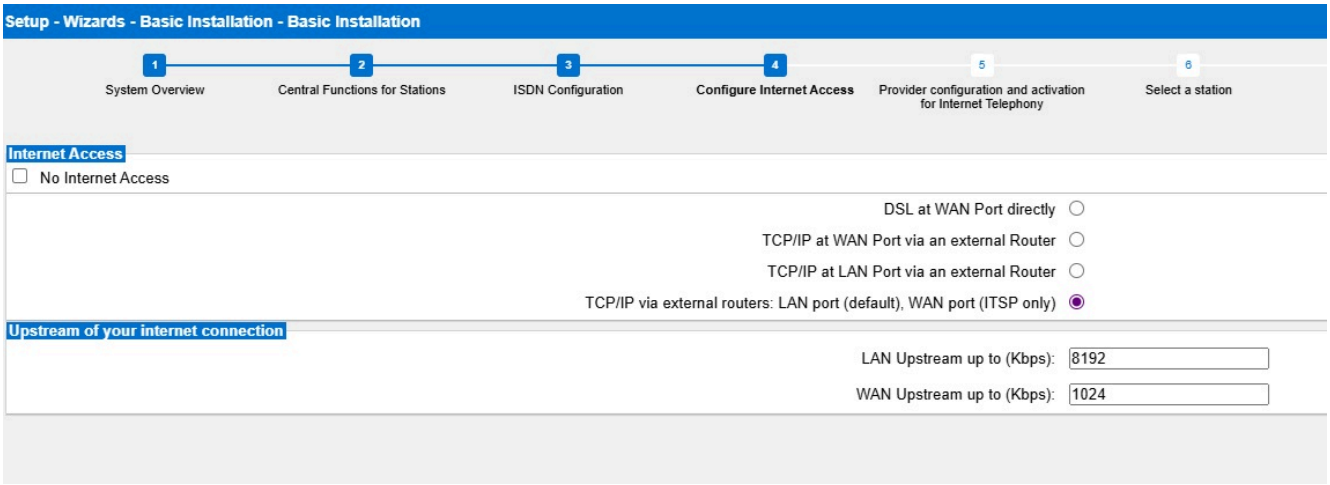
NOTICE: Calls can also be conducted via an Internet Telephony Service Provider; see Internet Telephony.

---

2) Click on **OK & Next**.

5.7.5 Internet Access

The **Configure Internet Access** window can be used to configure Internet access.



The configuration of Internet access in the WBM depends on whether the Internet connection has already been set up in an external router or whether it occurs via an Internet modem and thus needs to be set up in the WBM.

Only one of the options listed here may be selected.

- Internet access through an Internet modem (**DSL at WAN port directly**)

  You want to operate the communication system directly at an Internet modem (DSL, cable, UMTS ...). OpenScape Business has the Internet router integrated. Enter the access data of the Internet Service Provider (ISP) directly in the communication system and use the WAN port of the communication system.



You have the following options:

– **Internet access via a preconfigured ISP**
– **Internet access via the standard ISP PPPoE**
– **Internet access via the standard ISP PPTP**

If your ISP is not listed under the pre-configured ISPs, use the default ISP PPPoE or PPTP.

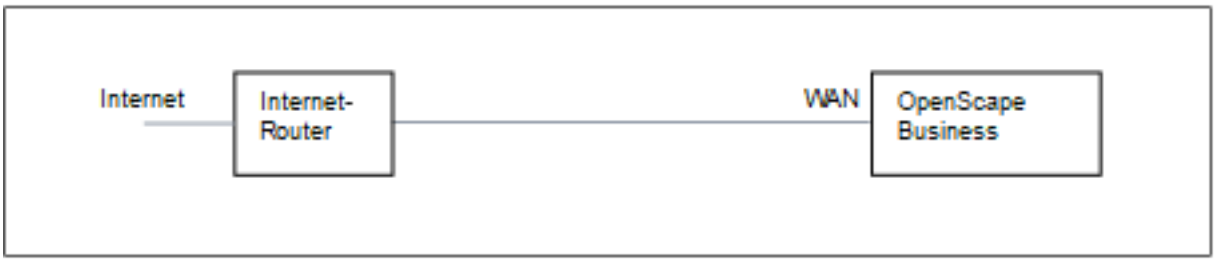
- Internet access via an external Internet router

  You want to operate the communication system at an external Internet router. The Internet Service Provider is already configured in the Internet router.

  You have the following options:

  – **Internet access via an external Internet router at the WAN port**

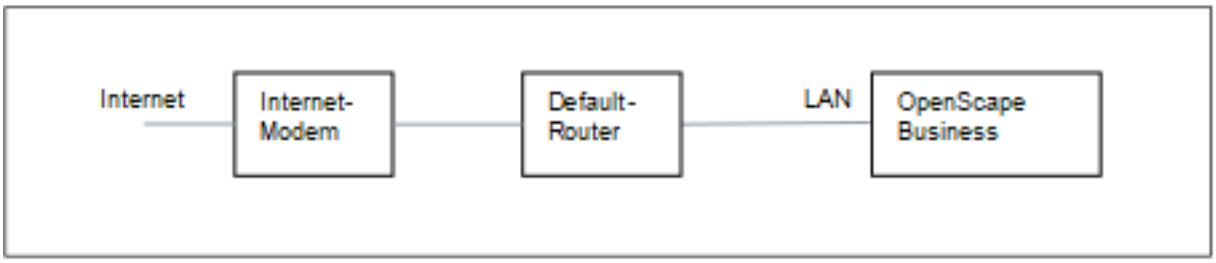
    (**TCP/IP at WAN port via an external router**)



  To do this, you use the WAN port of the communication system. OpenScape Business either knows the Internet router or works as a DHCP client. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

  – **Internet access via an external Internet router at the LAN port**

    (**TCP/IP at LAN port via an external router**)

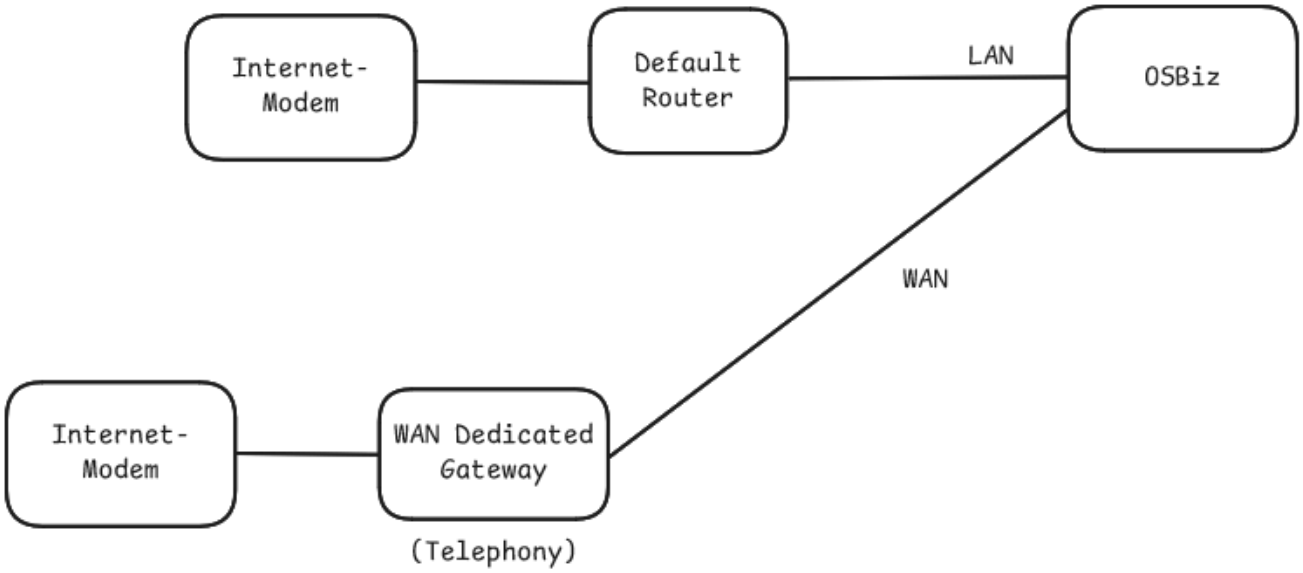


  To do this, you use the LAN port of the communication system. OpenScape Business knows only the default router and not the underlying infrastructure. To activate the connection to the Internet router,

the IP address of the default router and that of the DNS server must be made known to the communication system.

– **Internet access via an external Internet router at the LAN port**

(**TCP/IP at LAN/WAN port via an external router with WAN port dedicated to ITSP**)



To do this, you use the LAN port of the communication system, while the WAN port is dedicated to the ITSP. OpenScape Business knows only the default router and not the underlying infrastructure. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.

- Deactivate Internet access (default setting)

  You do not want to use the Internet.

NOTICE: STUN is not supported on the WAN interface when using the LAN/WAN feature. It is supported only on the LAN interface. If the ITSP requires STUN, SIP traffic must be routed through the LAN interface.

5.7.5.1 How to Configure Internet Access via an External Internet Router over the LAN Port

Prerequisites

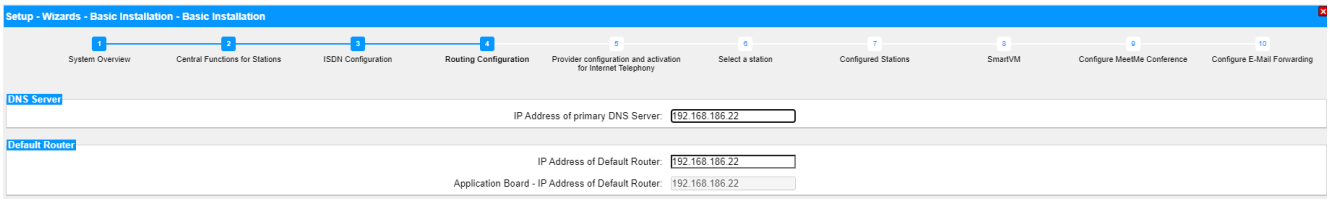
The communication system must be connected to the customer LAN via the "LAN" interface. The connection must not use the WAN port, since the WAN port will be disabled.

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

Step by Step

1) Disable the **No Internet Access** check box.

2) Activate the radio button **TCP/IP at LAN Port via an external router**, enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field and click **OK & Next**.



3) Enter the IP address of the local DNS server (e.g., the Internet router) or the Internet DNS server (for Internet telephony, for example) in the **IP address of the preferred DNS server** field.
4) Enter the IP address of the external Internet router in the **IP Address of Default Router** field.
5) Click on **OK & Next**.

5.7.5.2 How to Configure Internet Access via an External Internet Router over the WAN Port

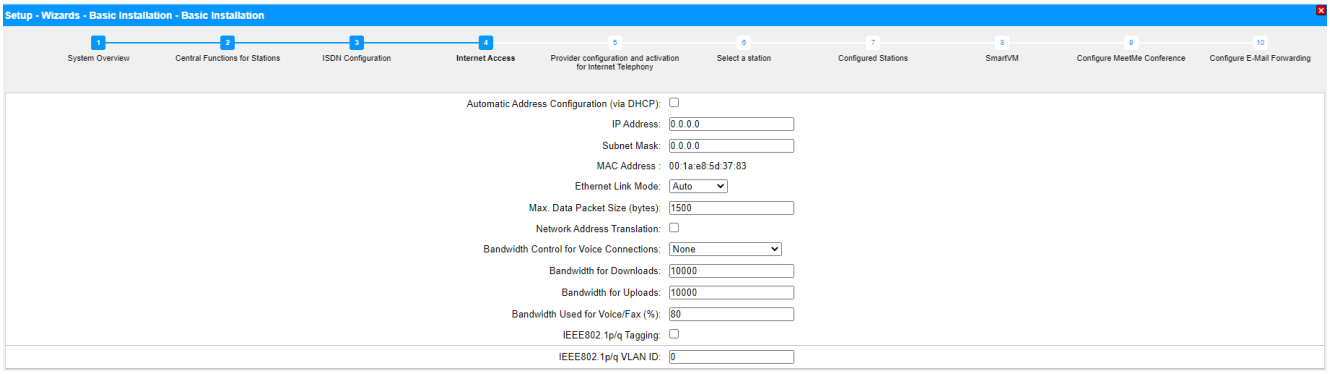
Prerequisites

The communication system must be connected to the LAN segment of the customer LAN in which the Internet router is located via the LAN interface "WAN".

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **TCP/IP at WAN Port via an external router** and click **OK & Next**.



3) If the network-specific data for the WAN interface are to be obtained from an already active DHCP server:
   a) Select the check box **Automatic Address Configuration (with DHCP)**.
   b) Select the **Accept IP Address of the Default Router** check box if you want this IP address to be used.
   c) Select the check box **Accept IP Address of the DNS Server** if required.
   d) Select the check box **Accept IP Address of the SNTP Server** if required.
4) If a fixed IP address is to be assigned to the WAN interface:
   a) Clear the check box **Automatic Address Configuration (with DHCP)**.
   b) Enter the desired **IP address** and **Netmask** of the WAN interface.
5) Enable the **NAT** check box.
6) If you also want to use Internet Telephony, select the item **Upload only** or **Upload and Download** as needed from the **Bandwidth Control for Voice Connections** drop-down list. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should only be activated for the upload direction to ensure that the download bandwidth reserved for voice transmission is not unnecessarily high.
7) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your Internet Service Provider.
8) Click on **OK & Next**.

5.7.5.3 How to Configure Internet Access via a Preconfigured ISP

Prerequisites

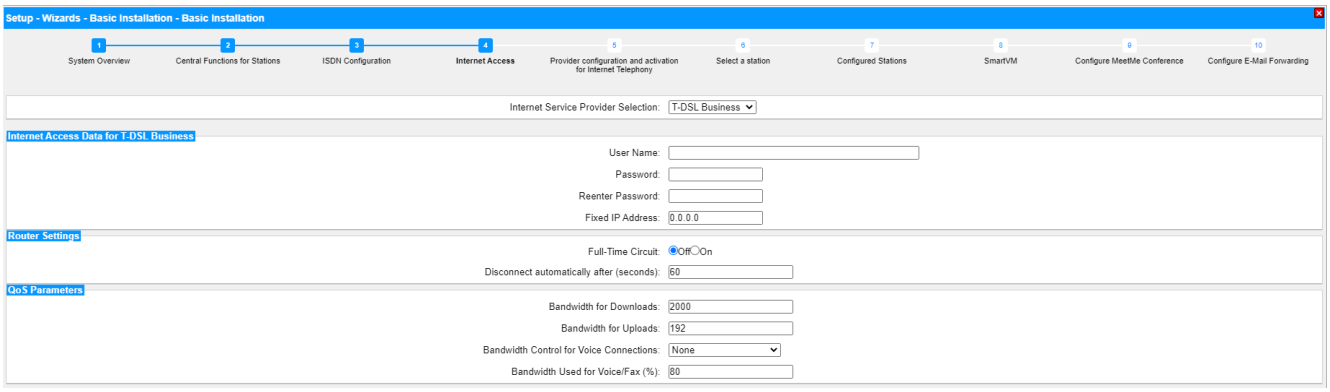
You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

Your ISP's Internet access data is available (for example, user account, password, bandwidth for upload and download, etc.).

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **DSL directly at Mainboard WAN Port** and click **OK & Next**.



3) Select your ISP from the **Internet Service Provider Selection** drop-down list.

4) Enter the access data that you received from your ISP in the **Internet Access Data for...** area. The fields in this area ate provider-specific. When entering your data, bear in mind that the input is case-sensitive!

5) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:

   - If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be interrupted (e.g., 01:30). Make sure that no data is exchanged with the Internet (e.g., software downloads or Internet telephony) during this time.
   - If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

6) Set the following values in the **QoS Parameters** area:

   a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

   b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

7) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

8) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).

   a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).

   b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

      `http://www.anydns.info/update.php?`
      `user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

   c) Enter the **User name** and the **Password** of your DynDNS account.

   d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.

   e) Test the DynDNS account with **Connection test**.

   f) After the test succeeds, click **OK**.

   g) Click **OK & Next**.

9) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

10) Click **OK & Next**.

5.7.5.4 How to Configure Internet Access via the Standard ISP PPPoE

Prerequisites

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.
3) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPPoE**.
4) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP**

Address Negotiation drop-down list, select the item **Use configured IP address**.

5) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:
   - If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be interrupted (e.g., 01:30). Make sure that no data is exchanged with the Internet (e.g., software downloads or Internet telephony) during this time.
   - If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).
6) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.
   - Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. The customary standard is the **CHAP Client** authentication mode.
   - Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.
7) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.
8) Set the following values in the **QoS Parameters of Interface** area:
   a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.
   b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).
9) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.
10) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).
   a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).
   b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

      `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
   c) Enter the **User name** and the **Password** of your DynDNS account.

d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.
e) Test the DynDNS account with **Connection test**.
f) After the test succeeds, click **OK**.
g) Click **OK & Next**.

11) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

12) Click **OK & Next**.

5.7.5.5 How to Configure Internet Access via a Standard ISP PPTP

Prerequisites

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
PPTP Parameter		
Local IP Address of the Control Connection	IP address that was assigned to you by your ISP for the PPTP connection. The default value is 10.0.0.140.	
Remote IP Address of the Control Connection	IP address of your ISP's server for the PPTP connection. The default value is 10.0.0.138.	
Remote Netmask for the Control Connection	Subnet mask that was assigned to you by your ISP for the PPTP connection. The default value is 255.255.255.248.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	

Field	Description	Value from ISP
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Optional: The data for a DynDNS account is available to you (name, password, host name, domain name of the DynDNS provider)

Step by Step

1) Disable the **No Internet Access** check box.
2) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.
3) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPTP**.
4) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP Address Negotiation** drop-down list, select the item **Use configured IP address**.
5) Enter the values that you received from your ISP in the **PPTP Parameter** area.
6) If you have a time-based tariff model, select the **Short Hold** check box. In the **Short Hold Time (sec)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).
7) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.
   - Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. Make the PAP and CHAP settings, as assigned to you by your ISP.
   - Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.
8) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.
9) Set the following values in the **QoS Parameters of Interface** area:
   a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.
   b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

10) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.
11) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).
    a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).
    b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

       `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
    c) Enter the **User name** and the **Password** of your DynDNS account.
    d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.
    e) Test the DynDNS account with **Connection test**.
    f) After the test succeeds, click **OK**.
    g) Click **OK & Next**.
12) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.
13) Click **OK & Next**.

5.7.5.6 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP

Prerequisites

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

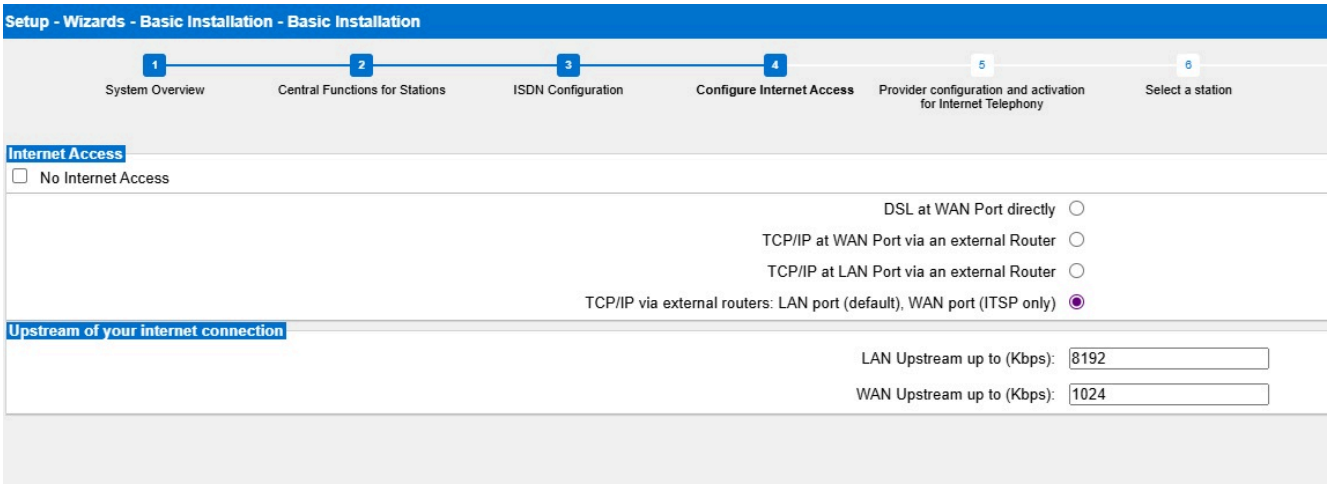
This feature is only applicable for ITSPs that do not require the use of STUN in the provider settings.

It is not possible to connect two identical ITSPs (with the same registrar/proxy) simultaneously via LAN and WAN.

Step by Step

1) Disable the **No Internet Access** check box.

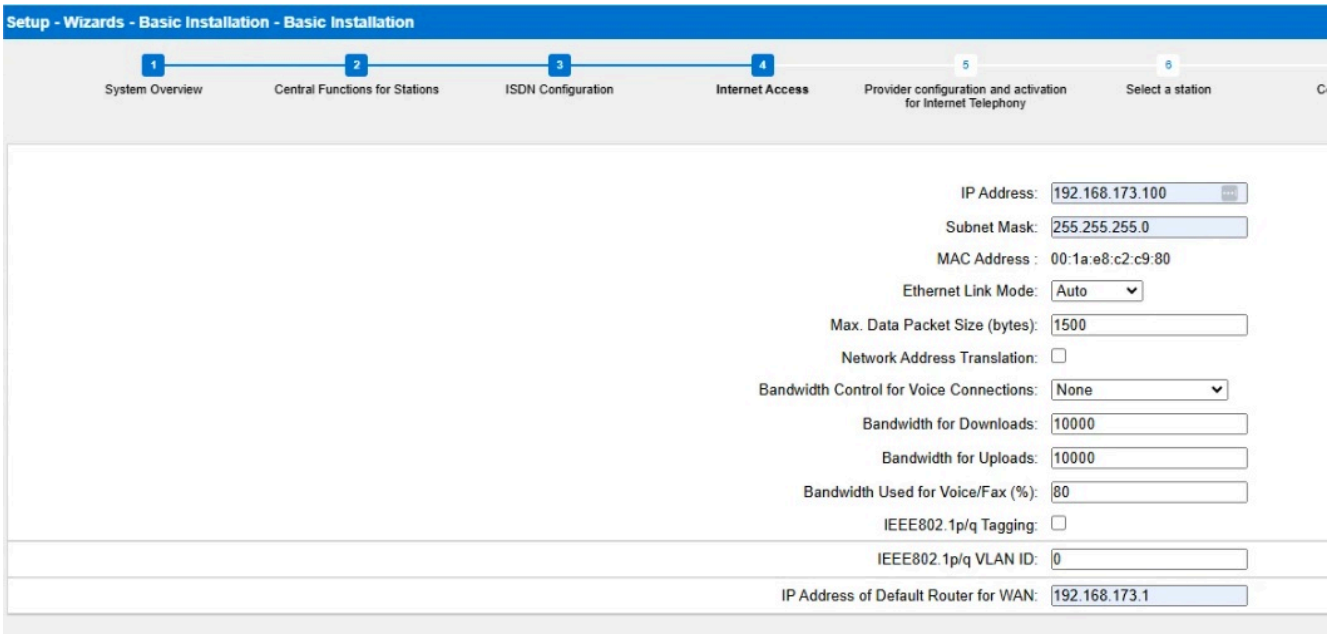
2) Activate the radio button **TCP/IP via external routers: LAN port (default), WAN port ITSP only**.



3) Configure the maximum upstream Kbps value for each interface in **LAN Upstream up to (Kbps)** and **WAN Upstream up to (Kbps)**.

4) Click on **OK & Next**.

5) Enter the WAN port IP configuration and additionally the IP address of the default router for the WAN port.



6) Click on **OK & Next**.

5.7.5.7 How to Disable Internet Access

Prerequisites

You are in the **Configure Internet Access** window of the **Basic Installation** wizard.

Step by Step

1) Leave the **No Internet Access** check box enabled.
2) Click on **OK & Next**.

5.7.6 Internet Telephony

The **Provider configuration and activation for Internet telephony** window is used to configure Internet telephony. You can configure predefined or new Internet Telephony Service Providers (ITSPs). You can configure one or several accounts for each ITSP. Up to 8 ITSPs may be active simultaneously.

You have the following options:

- **Configure a predefined ITSP**

  You can use predefined ITSP templates. To do this, the own access data and phone numbers are entered in the template, and this is then activated.
- **Configure a new ITSP**

  You can also add and activate a new ITSP.

  Configuring a new ITSP is seldom required and can be very time-consuming. This option is therefore not described in the initial installation. Detailed information can be found in the chapter Configuring an ITSP .
- **Disable Internet telephony**

  You can disable Internet telephony.

NOTICE: Configuration examples can be found on the Internet at the **Unify Experts Wiki** under *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Assigning the ITSP Phone Numbers

- In the case of an **Internet Telephony Station Connection**, the ITSP provides individual numbers such as 70005555, 70005556, etc. These individual call numbers are then assigned manually as the internal call numbers of the subscribers.
- In the case of an **Internet telephony point-to-point connection**, the ITSP provides a call number range, e.g., (+49) 89 7007-100 to (+49) 89 7007-147. The call numbers from the range are then assigned manually as the internal call numbers of the subscribers.

These two connection types can be combined as appropriate.

Alternatively, the ITSP phone numbers can be entered as the DID call numbers of the subscriber for both connection types during the station configuration.

Internal call number	Name	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

The ITSP call numbers thus result from the configured PABX number (e.g., country code 49) and the entered DID numbers in long format. This has advantages for the digit analysis and call management, even in an internetwork. The ITSP connection is thus DID-enabled for another node, for example.

A further CO trunk connection via ISDN is only possible to a limited extent in this case (useful for emergency calls, for example).

5.7.6.1 How to Configure a Predefined ITSP

Prerequisites

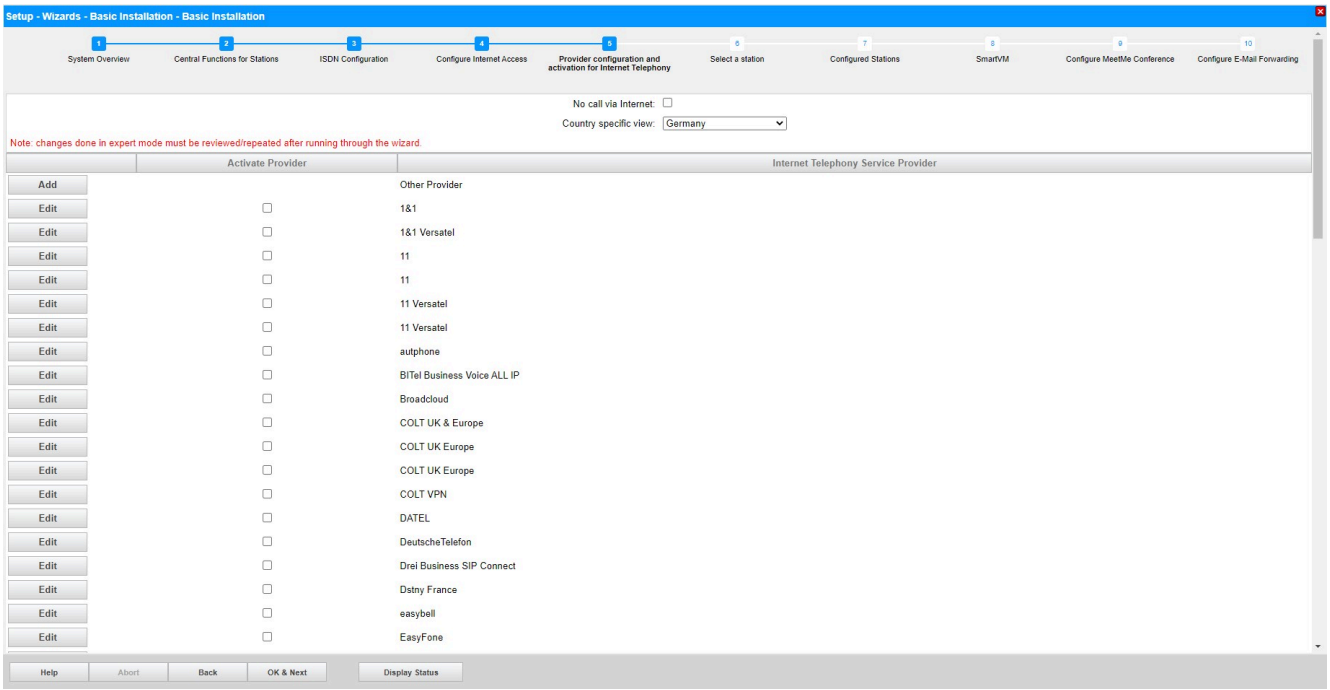
You are in the **Provider configuration and activation for Internet Telephony** window of the **Basic Installation** wizard.

The Internet connection is operational.

Your ITSP's Internet telephony access data is available (for example, user account, password and Internet telephony numbers).

Step by Step

1) Clear the **No call via Internet** check box. A country-specific list of the possible ITSPs is displayed. The list contains the predefined ITSPs for the selected country and any already created ITSPs.



2) If you want to change the preset country, select the desired country from the **Country specific view** drop-down list to display the ITSPs that are available for this country.

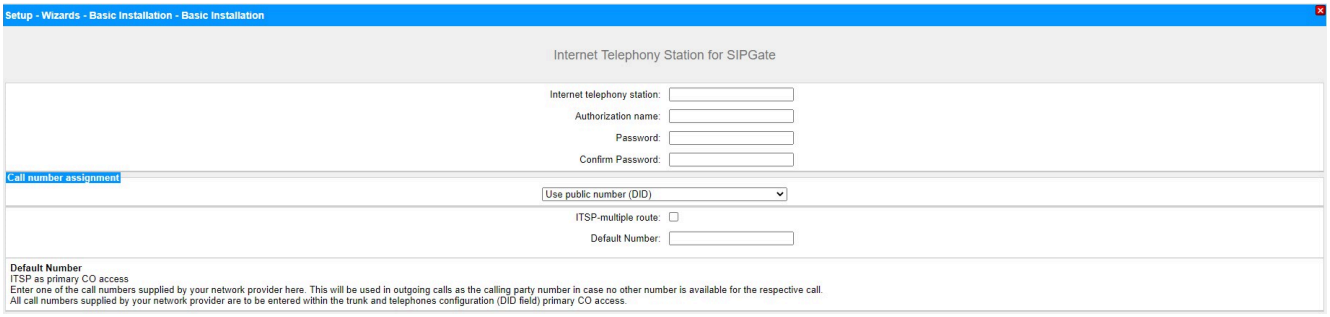
3) If required, click **Display Status** to check which ITSPs have already been activated and which Internet telephony subscribers have already been configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.

4) To configure Internet telephony stations, click **Edit** in the line associated with the relevant ITSP.

5) Activate the check box **Enable Provider**.

6) Click **OK & Next**.

7) Click **Add** to configure your ITSP accounts with the corresponding Internet telephony numbers. The fields that will then be displayed are provider-specific.



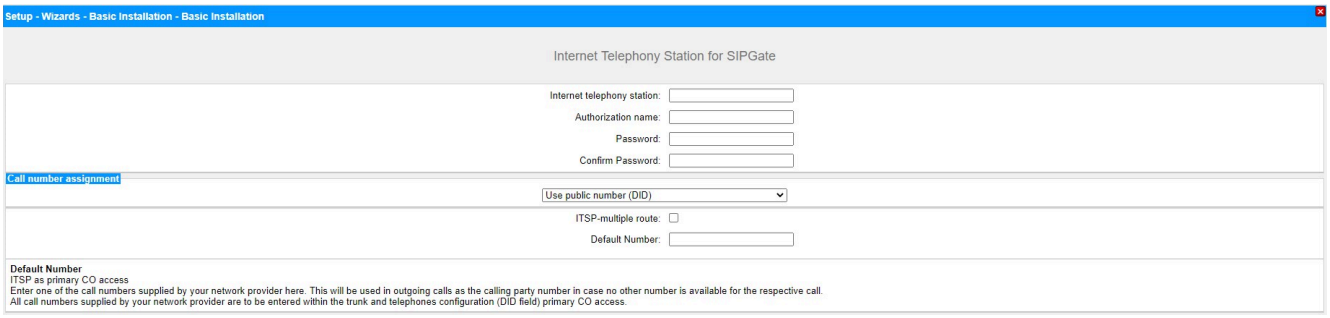
8) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

9) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

10) Enter the password you received from the ITSP in the **New Password** and **Confirm Password** fields. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

11) Assignment of Internet telephony phone numbers - Option 1:

Use public number (DID): the Internet telephony phone numbers of your Internet telephony station connection or Internet telephony point-to-point connection are not entered here during the ITSP configuration, but when the configuring the stations, i.e. the telephones and subscribers (in the **DID** fields).



a) Select the option field **Use public number (DID)** in the **Call number assignment** area.

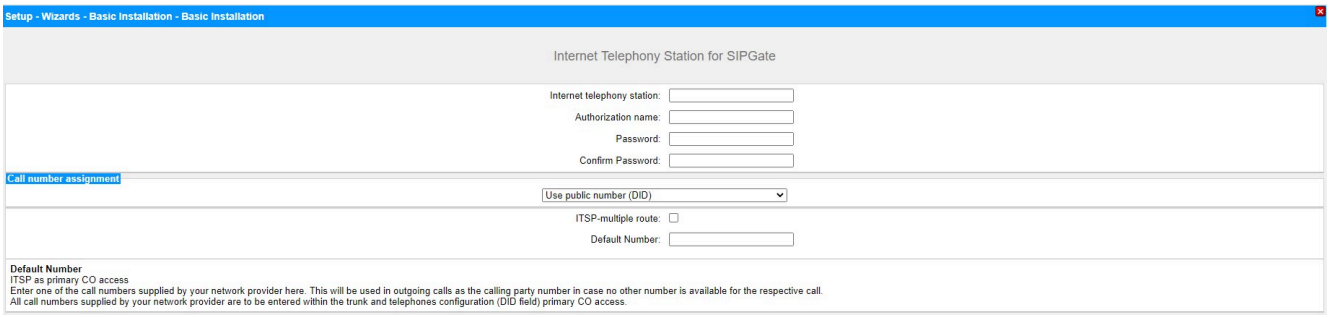
b) Under **Default Number**, enter the phone number to be used for outgoing calls when no caller DID number is available.

c) If your ITSP supports the "Mobile Extension (MEX)" feature, enter the MEX number provided by the ITSP (8 positions, digits only) under **MEX Number**.

12) Assignment of Internet telephony phone numbers - Option 2:

Use internal number (CalIno) / Single entries: You have an Internet telephony station connection and have received individual call numbers

as Internet telephony phone numbers (e.g. 70005555, 70005556,...). Then assign these single numbers to the internal call numbers of the subscribers.



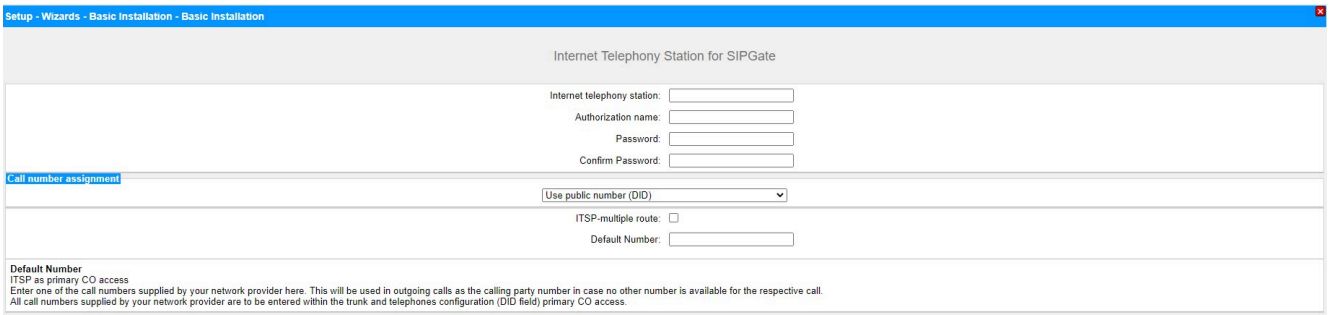
a) Select the option field **Use internal number (CalIno) / Single entries** in the **Call number assignment** area.

b) In the **Internet Telephony Phone Numbers** area, enter one of the Internet telephony phone numbers provided by the ITSP in the field next to the **Add** button and then click **Add**.

c) To assign further Internet telephony numbers to the account, repeat step b).

13) Assignment of Internet telephony phone numbers - Option 3:

Use internal number (CalIno) / Range entry: You have an Internet telephony point-to-point connection and have received a call number range as Internet telephony phone numbers (e.g., +49) 89 7007-100 to (+49) 89 7007-147. You then assign the call numbers from the call number range as the internal call numbers of the subscribers.



a) Select the option field **Use internal number (CalIno) / Range entry** in the **Call number assignment** area.

b) Enter the system phone number under **System phone number (prefix)**.

c) Enter the desired DID number range for the Internet telephony station in the 'from' **and** 'to **' fields after** Direct inward dialing band. The range entered by default is 100 - 147.

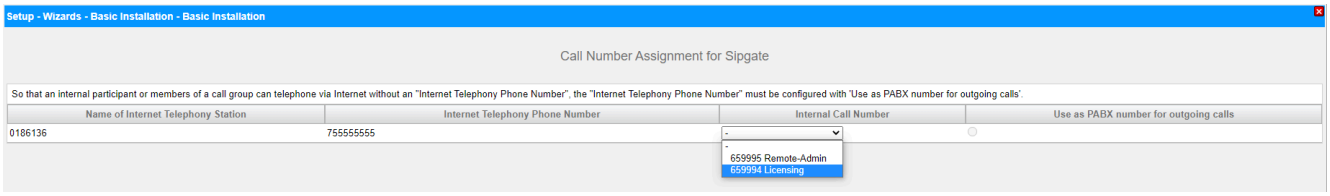
14) Click on **OK & Next**.

15) If you want to configure additional accounts and their associated Internet telephony numbers, repeat steps 7 through 14.

16) Click **OK & Next**. You will see an overview of which Internet telephony phone numbers are assigned to accounts.

17) Assign one internal station number each to every Internet telephony phone number.

This step is not required if you have selected option 1 for the assignment of the Internet telephony phone numbers. In this case, the assignment is made when the configuring the stations (i.e., the telephones and subscribers) in the **DID** field.



a) To do this, select an internal call number in the appropriate line from the **Internal Call Number** drop-down list.

b) If subscribers without Internet telephony phone numbers or members of a call group are to be allowed to make external calls via the Internet, the radio button **Use as PABX number for outgoing calls** must be activated. The radio button can be activated for only one single Internet telephony phone number.

18) Click **OK & Next**. Here you see again the list of predefined and newly added ITSPs. The enabled ITSPs are identified with a check mark in the **Enable Provider** column. If you are having connection problems with already activated ITSP, you can register it again with **Restart ITSP**.

19) Click **OK & Next**.

20) Enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field. Please do not confuse this with the download speed!

NOTICE: The number of simultaneous Internet calls permitted is displayed in the **Number of Simultaneous Internet calls** field. If the voice quality deteriorates due to the network load, you will need to reduce the number.

For more information about the number of simultaneous Internet calls, please refer to Limiting the Number of Simultaneous Calls via an ITSP on page 781.

---

21) Click **OK & Next**.

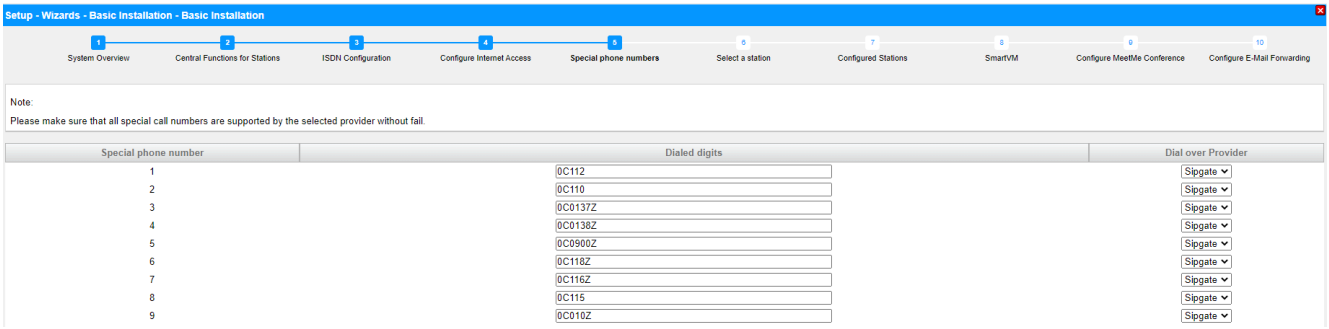
22) If you did not activate the full-time circuit when setting up your Internet access, you can now do this here. Without a permanent connection (full-time circuit), you cannot receive calls over the Internet. If the full-time circuit has already been set up, the fields described under a) to c) will not appear.

a) Enable the radio button **On** under **Full-Time Circuit**.

b) In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be deactivated (e.g., 04:59).

c) Click **OK & Next**.

23) Enter the special numbers you want in the **Dialed digits** column.



The following station number entries are valid:

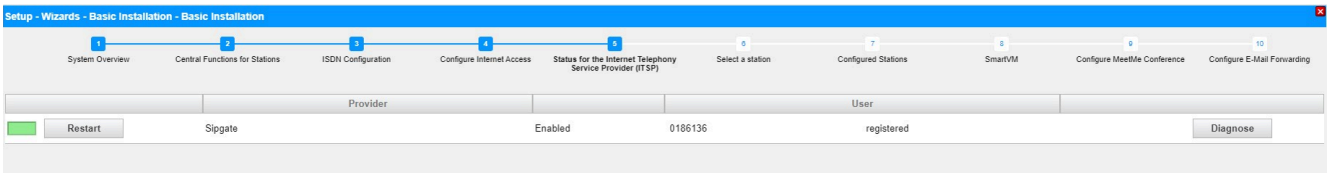
- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

24) Use the **Dial over Provider** column to specify whether the special number should be dialed via ISDN or an ITSP. Only the active ITSP is displayed.

NOTICE: Ensure that emergency numbers can always be dialed. If you want to dial emergency numbers via an Internet Telephony Service Provider, you must make sure that the ITSP supports this feature.

---

25) Click **OK & Next**. The status of your ITSP will be displayed.



The configured ITSPs at which you are already registered are marked in green.

The configured ITSPs at which you are not yet registered are marked in orange.

26) Click **Next** followed by **Finish**.

5.7.6.2 How to Deactivate Internet Telephony

Prerequisites

You are in the **Provider configuration and activation for Internet Telephony** window of the **Basic Installation** wizard.

Step by Step

1) Leave the **No call via Internet** check box selected.

2) Click **OK & Next** twice.

5.7.7 Stations

In the **Select a station - ...** window, you can configure the stations connected to the communication system.

Proceed as follows:

1) Configure ISDN stations

ISDN stations include ISDN phones or ISDN fax devices, for example. ISDN stations can only be configured if an S_0 interface has been set up as the internal S_0 port.

2) Configure analog stations

Analog stations include analog phones or analog fax devices, for example.

3) Configure UP0 stations

UP0 stations include system phones such as OpenStage 60 T.

4) Configure DECT stations

DECT stations are Cordless/DECT phones. DECT stations can only be configured if one or more Cordless base stations are connected and if the DECT phones have been registered at the base stations. Manager E is used to perform the configuration. For more detailed information on the Cordless configuration, see Configuring the Integrated Cordless Solution

5) Configure the IP and SIP stations

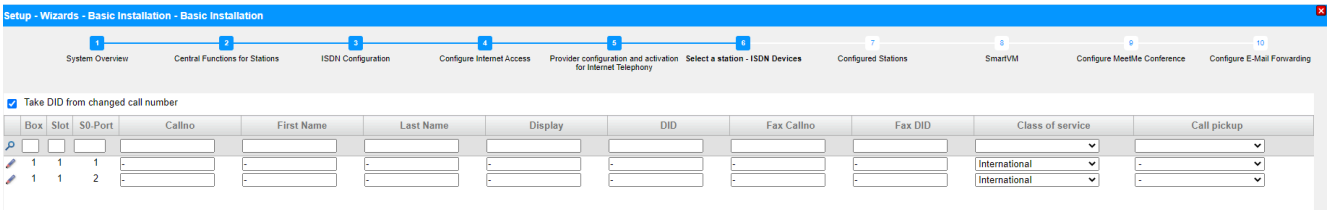
IP and SIP stations include LAN phones or WLAN phones, for example.

5.7.7.1 How to Configure ISDN Stations

Prerequisites

You are in the **Select a station - ISDN Devices** window of the **Basic Installation** wizard.

The S_0 ports to which the ISDN phones are to be connected must be configured as internal S_0ports.



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:
   - Only for a point-to-point connection:

     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

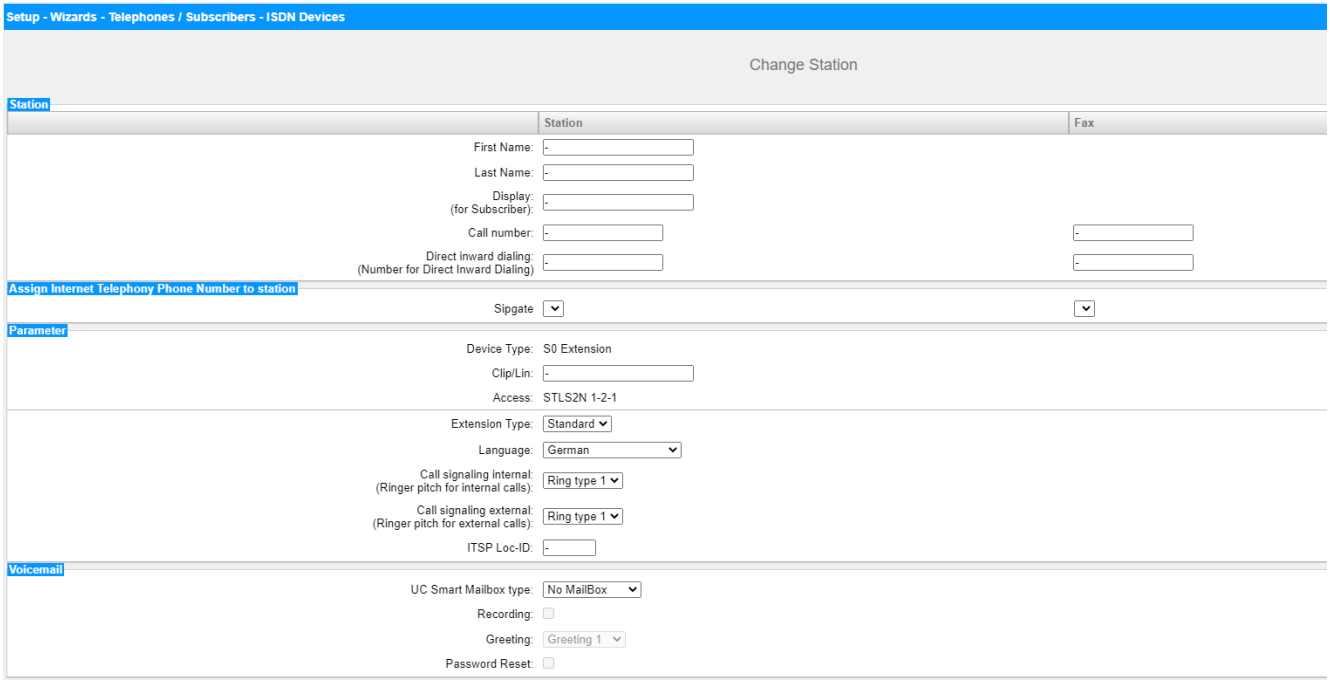
     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.
2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.
3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

   NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.
4) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:
   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.
6) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

7) Make the settings described under this step only if needed:

a) Click in the row of the desired ISDN station on the pencil icon **Edit**.



b) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of ISDN terminal from the **Extension Type** drop-down list.

d) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations,

thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Click on **OK & Next**.

h) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

i) Click on **OK & Next**.

8) If you want to configure additional ISDN stations, click on **Store data** and repeat steps 1 through 7.

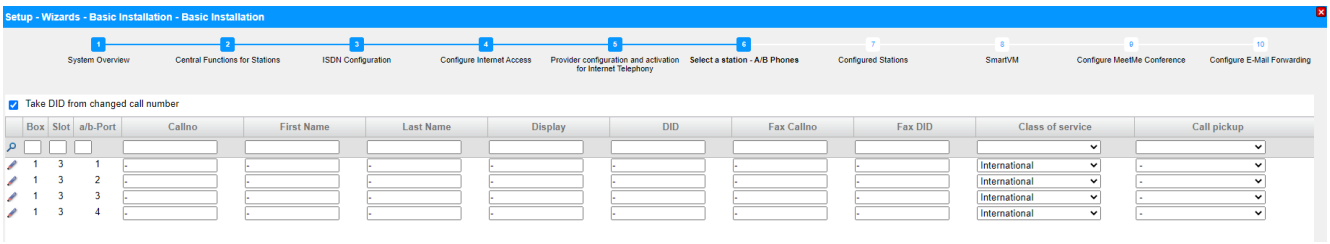
9) Click on **OK & Next**.

5.7.7.2 How to Configure Analog Stations

Prerequisites

You are in the **Select a station - A/B Phones** window of the **Basic Installation** wizard.

A mainboard or a board with analog interfaces is available.



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

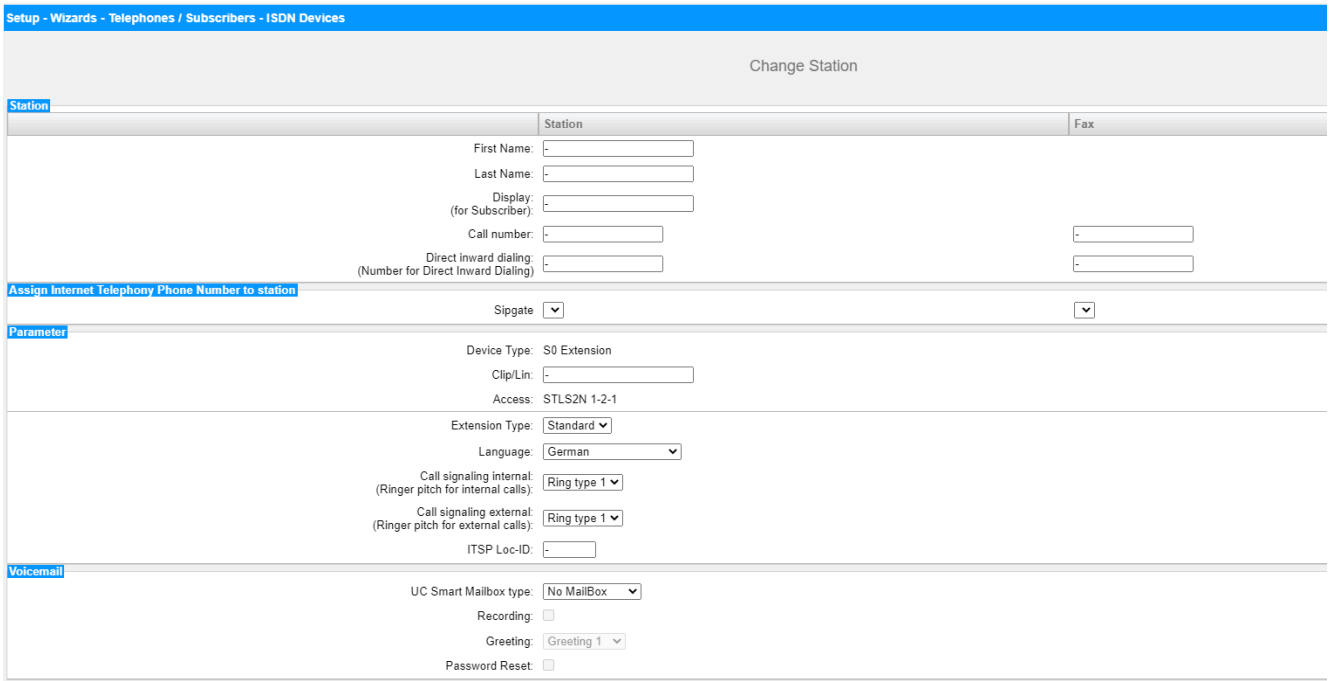
  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

4) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:
   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax DID** field in the row of the desired subscriber.
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.
6) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.
7) Make the settings described under this step only if needed:
   a) Click in the row of the desired analog station on the pencil icon **Edit**.



   b) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP

number and the internal call number is formatted and sent as the Calling Party Number for the external call.

c) Select the analog terminal type (Fax, for instance) from the **Extension Type** drop-down list.

d) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Click on **OK & Next**.

h) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

i) Click on **OK & Next**.

8) If you want to configure another analog station, click on **Store data** and repeat steps 1 through 7.

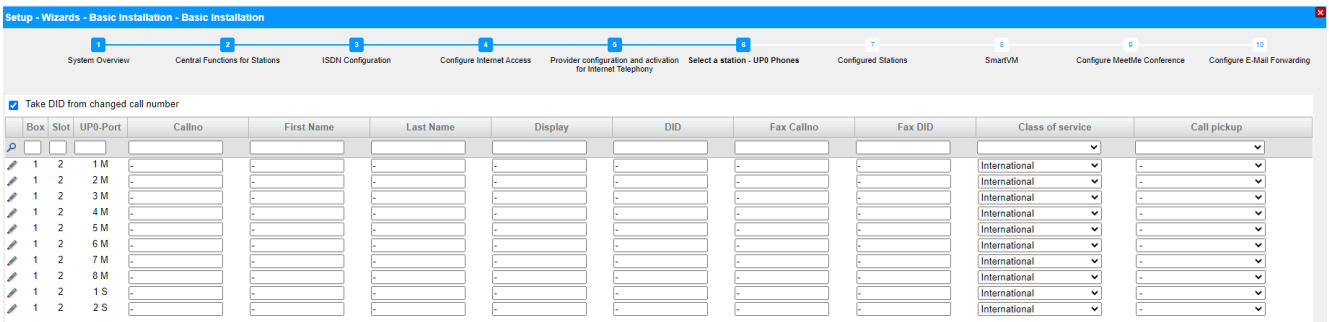
9) Click on **OK & Next**.

5.7.7.3 How to Configure UP0 Stations

Prerequisites

You are in the **Select a station - UP0 Stations** window of the **Basic Installation** wizard.

A mainboard or a board with UP0interfaces is available.



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

---

4) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

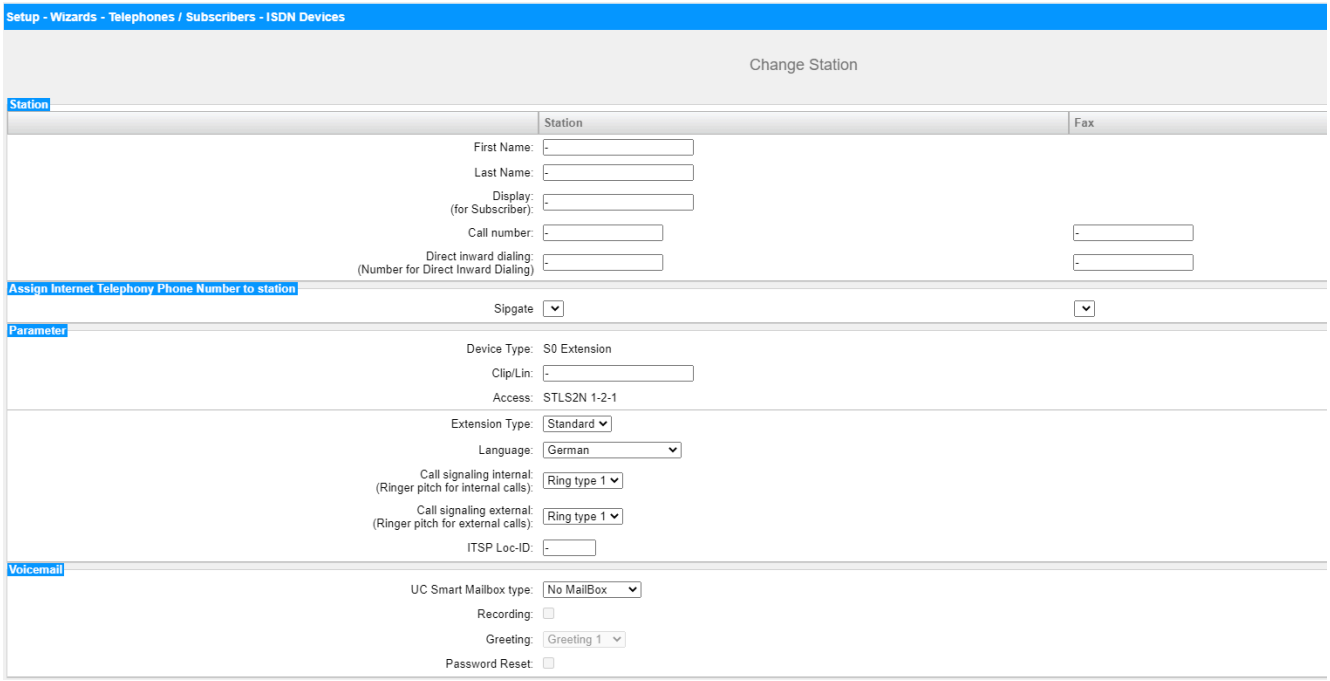
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

6) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

7) Make the settings described under this step only if needed:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of TDM terminal from the **Extension Type** drop-down list.

d) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for TDM terminals.

e) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

f) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations,

thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

g) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

h) Click on **OK & Next**.

i) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

j) Click on **OK & Next**.

8) If you want to configure another UP0 station, click on **Store data** and repeat steps 1 through 7.

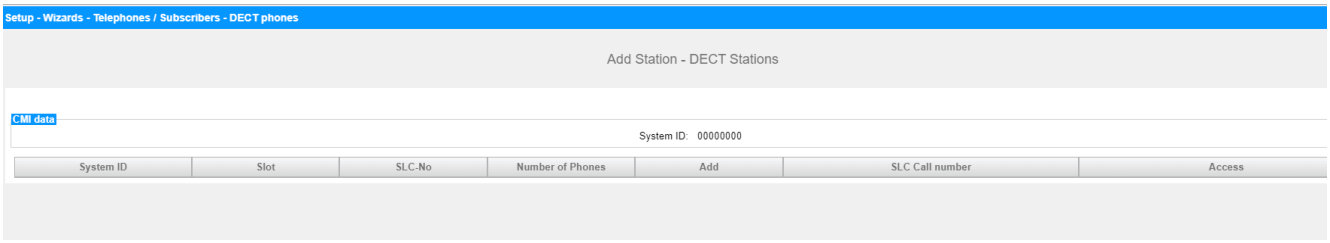
9) Click on **OK & Next**.

5.7.7.4 How to Configure DECT Stations

Prerequisites

You are in the **Select a station - DECT Stations** window of the **Basic Installation** wizard.

To configure DECT stations, a base station must be connected, and the DECT phones must be logged in there. If this is not the case, skip this window. You can also configure the DECT stations later (see Configuring Stations).



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:
   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

4) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

   NOTICE: The name can consist of up to 16 characters, but must not include any diacritical characters such as umlauts or special characters.

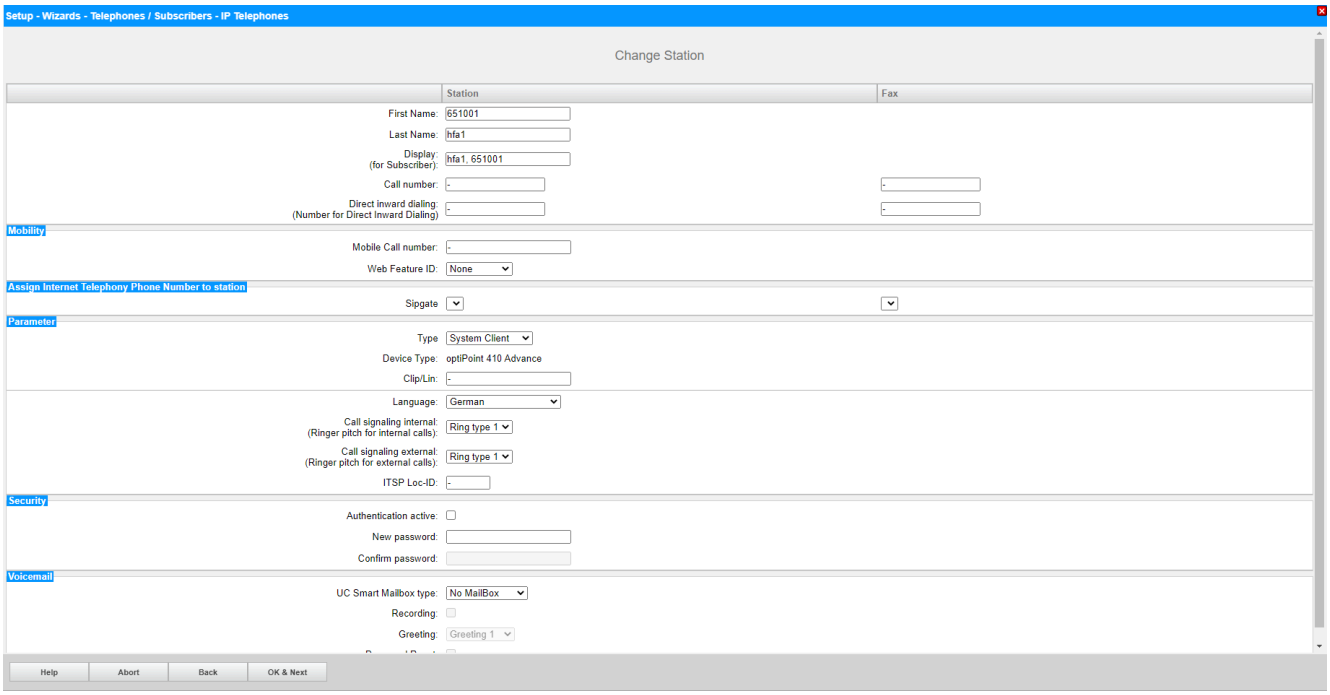
5) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

6) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

7) If you want to change the DECT phone code (PIN), enter the new code in the row of the desired subscriber under **Mobile code**. The DECT subscribers must log on at the base station again with this code.

8) Make the settings described under this step only if needed:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

c) Select the type of cordless device from the **Extension Type** drop-down list.

d) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for cordless devices.

e) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

f) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal

stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

g) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

h) Click on **OK & Next**.

i) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

j) Click on **OK & Next**.

9) If you want to configure another station, click on **Store Data** and repeat steps 1 through 8.

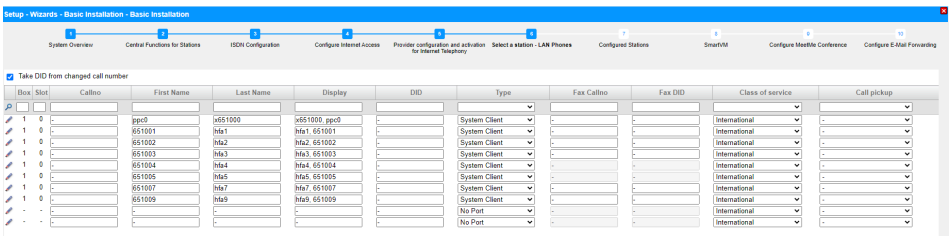
10) Click on **OK & Next**.

5.7.7.5 How to Configure IP and SIP Stations

Prerequisites

You are in the **Select a station - LAN Phones** window of the **Basic Installation** wizard.

A functional wireless LAN network is needed to operate WLAN phones.



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name`.

> **NOTICE:** The name can consist of up to 16 characters, but should not include any diacritical characters such as umlauts or special characters. The name specified here will be entered as the Last Name at the UC clients, but can be edited there.

4) Select the type of IP station (e.g., "System Client" or "SIP Client") from the **Type** drop-down list in the row of the desired station.

5) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

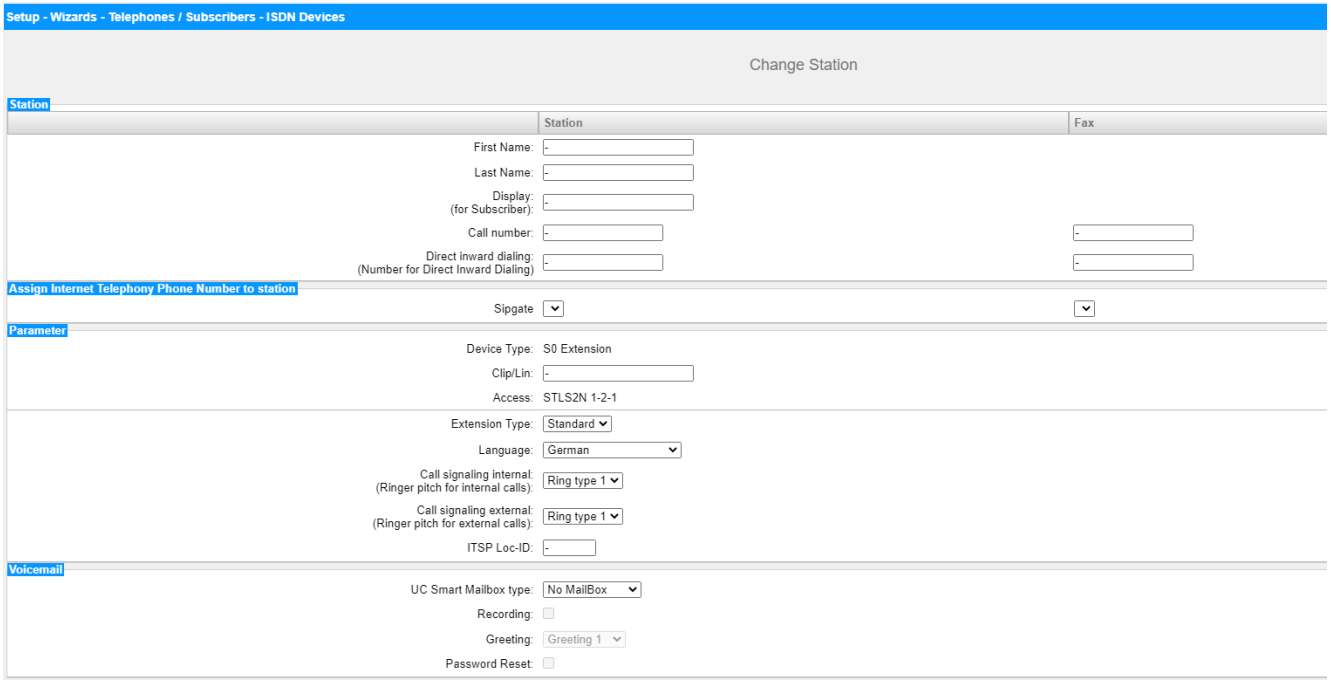
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

6) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

7) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

8) Make the settings described under this step only if needed or for a SIP phone:

   a) Click in the row of the desired station on the pencil icon **Edit**.



   b) For SIP phones: If the SIP phone is to be operated in conjunction with a dual-mode mobile phone, enter the dialout prefix followed by the telephone number of the mobile phone (e.g., **0016012345678**) in the **Mobility** area under `Mobile phone number`. In addition, select this

SIP client from the **Web Feature ID** drop-down list. (see Dual-Mode Telephony).

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

d) Select the language for the menu controls on the phone from the **Language** drop-down list.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Only for SIP phones: Enter the authentication password in the **Password** and **Confirm password** fields.

h) Only for SIP phones: Enter the user ID for the authentication in the **SIP User ID / Username** field.

i) Only for SIP phones: Enter the associated zone for the authentication in the **Realm** field.

j) Click on **OK & Next**.

k) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

l) Click on **OK & Next**.

9) If you want to configure another IP station, click on **Store data** and repeat steps 1 through 8.

10) Click on **OK & Next**. A list of all configured stations appears. This list is effectively a dial plan.

11) If required, click **Print** to print out the data of the configured stations.

12) Then click **OK & Next**.

Related concepts

Multilingual Text Output on page 1172

5.7.8 Configuring UC Suite

You can perform the automatic configuration of the UC solution UC Suite in the **Automatic Configuration of the Application Suite** window.

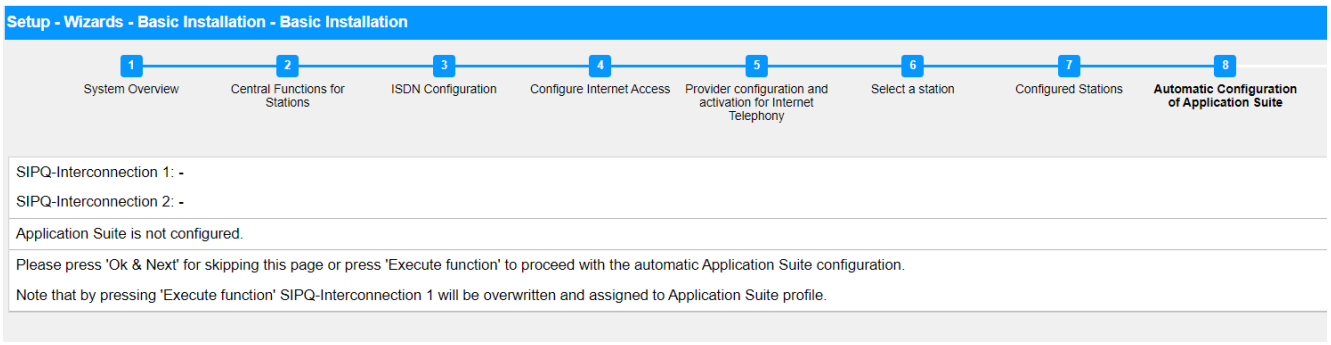
NOTICE: This window appears only if **Package with UC Suite** was selected during the application selection in the **Initial Installation** wizard.

The automatic configuration of the UC solution UC Suite requires a number of free trunk lines which will be statically occupied for the application. This number depends on system specification capacities and is listed in section Maximum values for lines on page 1370 (see *MEB Trunk channels for UC Suite* in the tables). In case the overall limit of 250 trunks is exceeded, the configuration of the UC Suite is not possible.

5.7.8.1 How to Configure the UC Suite

Prerequisites

You are in the **Automatic Configuration of Application Suite** window of the **Basic Installation** wizard.



Step by Step

1) If no UC Booster Card is integrated into the communication system, click on **OK & Next**. The configuration will be skipped.
2) If the UC Booster Card is integrated into the communication system, click on **Execute function**. The UC Suite is configured automatically. Once the progress bar shows 100%, click on **OK & Next**.

NOTICE:

For OpenScape Business X the wizard automatically generates 76 media channels.

5.7.9 Configuring UC Smart Mailboxes

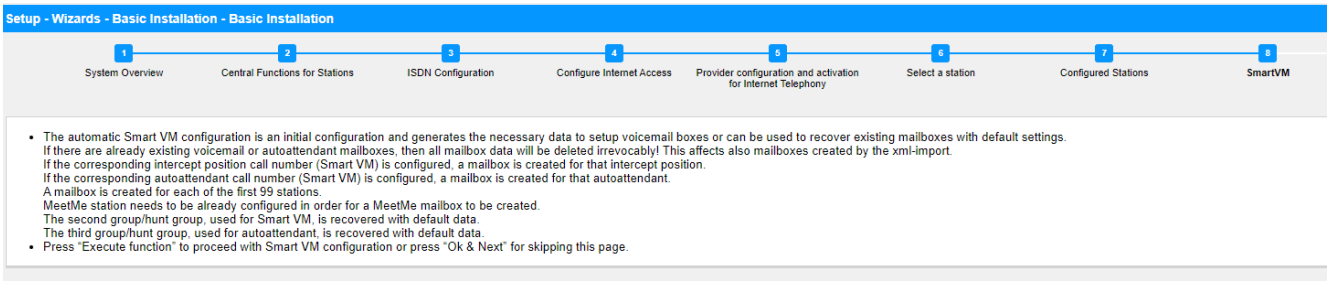
If you are using the UC solution UC Smart, you can perform the automatic configuration of the UC Smart voicemail boxes (Smart VM, Smart VoiceMail) in the **Automatic Configuration of Smart VM** window.

NOTICE: This window appears only if **Package with UC Smart** was selected during the application selection in the **Initial Installation** wizard.

5.7.9.1 How to Configure UC Smart Voicemail Boxes

Prerequisites

You are in the **Automatic Configuration of Smart VM** window of the **Basic Installation** wizard.



Step by Step

1) If the UC Smart voicemail boxes are not to be used, click on **OK & Next**. The configuration of the voicemail boxes will be skipped.
2) If the UC Smart voicemail boxes are to be used, click on **Execute function**. Voicemail boxes are then automatically configured for the first 100 subscribers. Once the progress bar shows 100%, click on **OK & Next**.

NOTICE: Existing UC Smart or UC Smart AutoAttendant voicemail boxes are irrevocably deleted in the process.

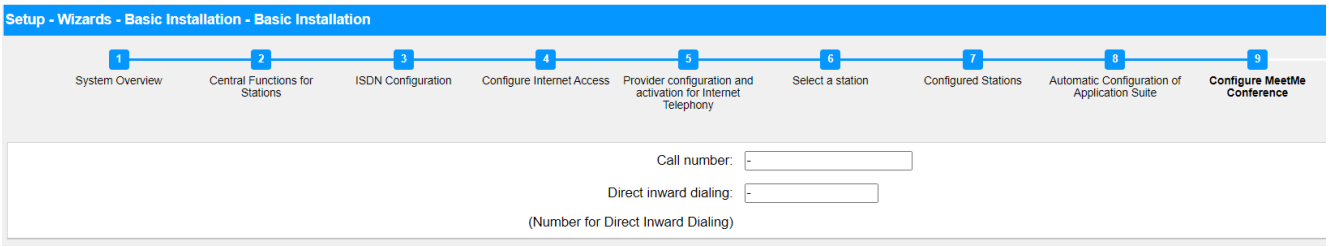
5.7.10 Conference Server Settings

The **MeetMe Conference** settings window can be used to define the call numbers and the dial-in numbers for conferences.

5.7.10.1 How to Edit the Conference Server Settings

Prerequisites

You are in the **Configure MeetMe Conference** window of the **Basic Installation** wizard.



Step by Step

1) Enter a phone number for the conference in the **Phone Number** field.
2) Enter the dial-in number for the conference (conference DID) with which subscribers can dial into an existing conference in the **Direct inward dialing** field.
3) Click on **OK & Next**.

5.7.11 E-mail Delivery (Optional)

You can configure the delivery of e-mails in the **Configure E-Mail Forwarding** window. These e-mails notify users of voicemail and fax messages and administrators of system messages.

You have the following options:

- Configuring the Sending of E-mails

  You can specify an external E-mail server via which the e-mails are to be sent by OpenScape Business. Voicemails, fax messages and internal system messages can then be sent via this E-mail server to one or several different configurable e-mail addresses.

NOTICE: Entering the e-mail server is important if an e-mail with a link to the installation file(s) is to be automatically sent to the users of the UC Suite.

5.7.11.1 How to Configure the Sending of E-mails

Prerequisites

If the external E-mail server has been configured to use basic authentication, make sure an e-mail account with a password exists with an e-mail provider, and you know the access data for this account.

If the external E-mail server has been configured to use modern authentication (Microsoft OAuth 2.0 token-based authorization), as in the case of Exchange Online, make sure that:

- The sender's email account must be allowed to use Authenticated SMTP (by default this option is inactive in Microsoft 365 tenant). Once Authenticated SMTP is activated, the OAUTH 2.0 email forwarding works normally with all OpenScape Business mainboards.

- An application with the required permissions has been registered in Microsoft Azure Active Directory (Azure AD) for your OpenScape Business system to send emails.
- You know the Application (client) ID and the Directory (tenant) ID of the registered application.

  Ask your Azure AD administrator to provide these values, if required.
- The email address that will appear as the sender of the emails belongs to the same Azure AD or tenant as the registered application.

You are in the **Configure E-Mail Forwarding** window of the **Basic Installation** wizard.

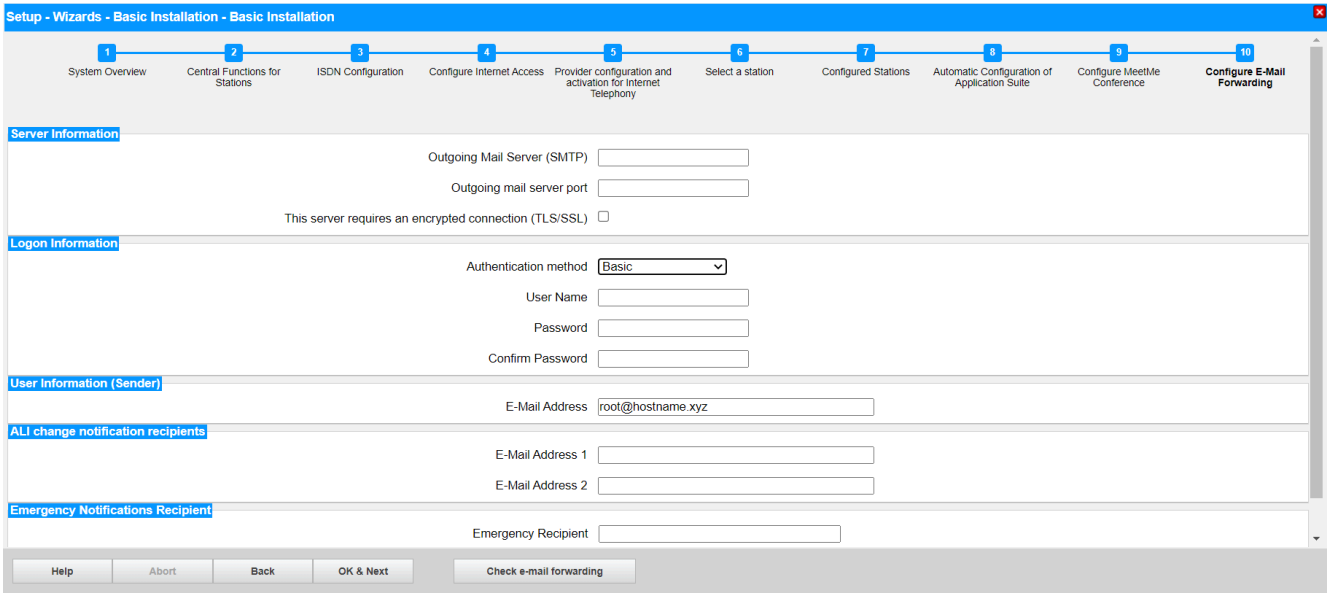


Figure 6: E-mail forwarding options when basic authentication method is selected

Step by Step

1) Enter the **Outgoing mail server (SMTP)** for the e-mail server to be used for sending e-mails, e.g., `smtp.web.de`. Ask your e-mail provider for the outgoing mail server if required.

   NOTICE: Make sure that the name of the outgoing mail server can be resolved. If not, you must start the e-mail sending function via **Service Center** > **E-mail Forwarding** and then enter the IP address of the outgoing mail server instead of its name.

2) Enter the **Outgoing mail server port** for the server port to be used for sending e-mails. Ask your e-mail provider for the outgoing mail server if required.
3) If a secure connection is required, enable the **This server requires an encrypted connection (TLS/SSL)** check box. If required, check with your e-mail provider whether this option needs to be enabled.

4) If the external E-mail server has been configured to use basic authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Basic**.
   b) Enter the **User Name** of the e-mail account, e.g.,: `john.doe`.
   c) Enter the **Password** for the e-mail account and repeat it in the **Confirm Password** field.
5) If the external E-mail server has been configured to use modern authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Microsoft OAuth 2.0**.
   b) Enter the Application (client) ID obtained from the Microsoft Azure portal in the **Application ID** field.
   c) Enter the Directory (tenant) ID obtained from the Microsoft Azure portal in the **Tenant** field.
6) Enter the **E-mail Address** that will appear as the sender of the emails, for example: `john.doe@web.de`.
7) Enter the **E-mail Address 1** to get a notification email when ALI tolerance has been used. You may also enter a second email address in the **E-mail Address 2** field.
8) In the **Emergency Recipient** field, enter the e-mail address of an on-site security officer to which an e-mail is sent when an emergency number is dialed.

   The subject of the e-mail will be "New emergency call". The call number and the name of the caller, if configured, are included in the e-mail which are retrieved from the database of the system.
9) If you have selected **Microsoft OAuth 2.0** as authentication method, proceed as follows:
   a) Click on **OK & Next**.
   b) Wait for an authorization link and user code to appear.

      The authorization code expires after some minutes.
   c) Open the authorization link and enter the user code on the pop-up.
   d) Sign in with the email address you have entered in step 6 on page 197 (**E-mail Address**).

      The email address must be in the same Azure AD or tenant as the registered application.
   e) After successful authentication, the pop-up displays a message as below:

      `You have signed in to the <application-name> on your device. You may now close this window..`
   f) Close the pop-up and return to WBM. If the authentication was successful, you will see the message `The authentication was successful!.`

10) If you want to check the entered e-mail settings, proceed as follows:
    a) Click on **Check e-mail forwarding**.
    b) Under **Send to e-mail address**, enter the e-mail address of any e-mail box that you can access. The test e-mail will be sent to that e-mail address.
    c) Under **Subject in the e-mail**, enter a descriptive text so that you can identify the e-mail in your e-mail inbox.
    d) Click on **Send Test E-mail**. The e-mail settings are verified, and the e-mail is sent to the specified e-mail address.
    e) Check whether the e-mail has arrived in your e-mail inbox.
    f) If the e-mail was sent correctly, click **Back** and proceed to the next step.
    g) If the e-mail delivery failed, click **Back** and correct your e-mail settings.
11) Click on **OK & Next** followed by **Finish**. The basic installation is finished. Before you perform the backup mentioned in the wizard, you should activate the licenses.

5.8 Closing Activities

After the initial installation and the basic installation with the WBM have been completed, some important settings must still be made for the operation of OpenScape Business.

Proceed as follows:

1) Activate and assign licenses

   The licenses procured with OpenScape Business must be activated within a period of 30 days. The time period begins the next time you log on to the WBM. After this time period expires, the communication system will only operate in restricted mode. Once the licenses have been activated successfully, they must be assigned to the stations and lines. In a standalone system, system-wide features are enabled automatically upon activation.
2) Provision the UC Smart client for installation (only for UC Smart)
3) How to Provision the UC Suite Clients for Installation (for UC Suite only)

   The UC Suite clients are part of UC Suite. The installation files for the UC Client are accessible via the WBM and can be made available to the IP stations automatically or manually.

   In addition, the administrator has the option of performing a silent installation. The silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC Suite PC clients on a PC without requiring any further user inputs. For more information, see Silent Installation/Uninstallation for UC Suite PC Clients.
4) Perform a data backup

   All previous changes to OpenScape Business must be backed up. The backup can be stored as a backup set on a USB storage device or in the internal network.

5.8.1 How to Activate and Assign the Licenses

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

You know the LAC (License Authorization Code) for releasing the license and have a user ID and password for accessing the license server.

You need Internet access to connect to the license server.

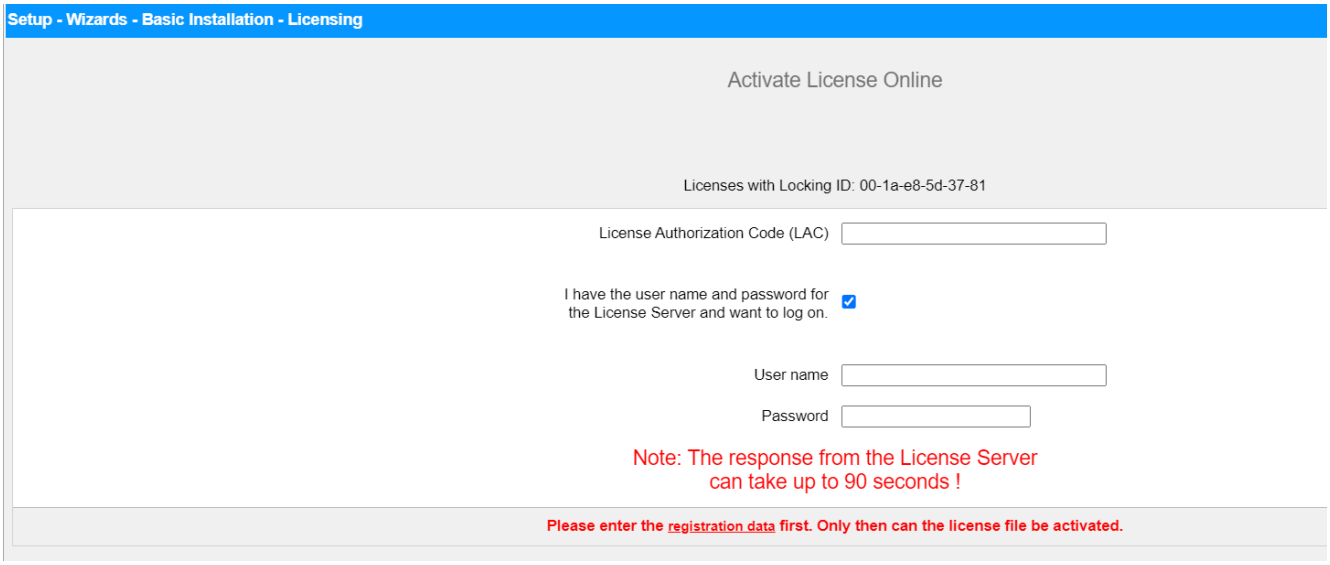
Step by Step

1) Activate license online:

a) In the navigation bar, click on **Setup**.

b) In the navigation tree, click **Wizards** > **Basic Installation**.

c) Click on **Edit** to start the **Licensing** wizard.



d) Enter the appropriate LAC in the **License Authorization Code (LAC)** field.

e) Select the check box **I have the user name and password for the License Server and want to log on**.

f) Enter the **User Name** and **Password** for logging into the License Server.

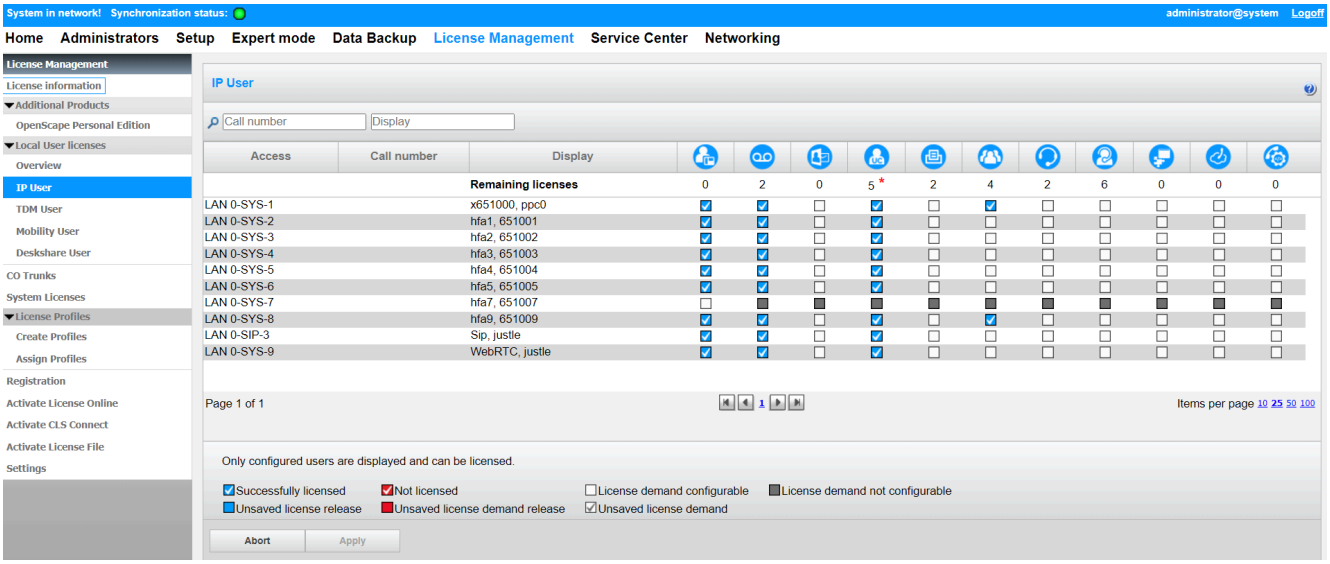
g) Click on **OK & Next**. The connection to the license server is established, and the licenses are released.

2) Assign licenses to stations:

a) Click on **License Management** in the navigation bar.

b) In the navigation tree, navigate to the desired type of subscriber under **Local User Licenses** > **...**. You will be shown a list of all subscribers of the selected subscriber type.

c) In the row of the desired subscriber, select the check box in the **User license** column (first column with check boxes).



d) Activate the user-oriented licenses in the row of the desired subscriber by selecting the appropriate check boxes.

NOTICE: User-oriented licenses can be assigned to a subscriber only if a station license (user license) was assigned to the subscriber earlier (step c).

---

e) Click on **OK & Next**. A check is performed to determine whether there are enough licenses for your assignment.

If sufficient licenses are available, the licensing of the subscriber is completed.

f) If licenses are missing, the errors are indicated by displaying a check box shaded in red. Correct these errors and repeat step e.

3) Assign licenses to trunks:
   a) In the navigation tree, click **CO trunks**. The number of trunk licenses purchased will be displayed in the **CO trunks** area.
   b) For SIP trunks: In the **License demand for number of simultaneous Internet calls in this node** area, enter the number of Internet calls that can be conducted simultaneously via an ITSP.
   c) For S_{2M} trunks: In the **S2M** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
   d) For T1 trunks (only for the U.S.): In the **T1** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
   e) Click on **OK & Next**.

NOTICE: The number of licensed SIP trunks and S_{2M}/ T1 trunks must not exceed the number of trunk licenses purchased.

5.8.2 How to Provision the UC Smart Client for Installation

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The hardware and software for using UC @work are available.

NOTICE: Licenses are required to use the UC Smart client myPortal @work.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Software** in the navigation tree.
3) Click on the Download icon of **myPortal @work** and save the installation file on a shared network drive.
4) Send the two installation files to the users of myPortal @work.
5) Alternatively, you can also send the users of myPortal @work the link with which they can access the installation file:

```
https://<IP address of the communication system>/
management/downloads/myPortalAtWorkSetup.exe
```

5.8.3 How to Provision the UC Suite Clients for Installation

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The hardware and software for using the UC Suite are available.

NOTICE: Licenses are required to use the UC Suite clients.

Step by Step

1) To enable the installation files to be provided automatically to a station, make sure that the following steps have been performed:
   a) The e-mail addresses of the stations and the associated subscriber data must have either been already imported via an XML file or entered later under **Setup** > **UC Suite** > **User Directory**.
   b) An e-mail server must have been specified.

   NOTICE: You can also enter an E-mail server later under **Service Center** > **E-mail Forwarding**.

   All subscribers whose e-mail addresses are known receive an e-mail with a link to the installation directory of the UC clients and Getting Started Instructions. The installation folder also includes a Readme file with information on installing the software on client PCs.
2) If the required steps for automatic notification are not fulfilled, you can also make the installation files available manually. To do this, proceed as follows:
   a) Click on **Service Center** in the navigation bar.
   b) Click on **Software** in the navigation tree.
   c) Click on the desired UC client and save the zipped installation file on a shared network drive.
   d) Click in the navigation tree on **Documents** and select **User Documentation** from the drop-down list.
   e) Click on the documentation of the desired UC client and save the documentation file on a shared network drive.
   f) Send the zipped installation file and the documentation file to the users of the UC clients by e-mail or inform the users about the storage location of these files.
   g) The zip file with the installation files also includes a Readme file. Notify the users that the installation of the UC clients must be performed in accordance with the installation notes in the Readme file.
3) Alternatively, you can also send the UC users links through which they can directly access the installation files of the UC clients.
   a) Click on **Service Center** in the navigation bar.
   b) Click on **Software** in the navigation tree.
   c) Click on the **Show Application Links** button. You will be presented with multiple links, depending on the used operating system and the desired UC client. For example:

   ```
   https://<IP address of the communication system>/
   management/downloads/install-common.zip
   ```

5.8.4 How to Perform a Data Backup

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

For a backup to a USB storage device (USB stick or USB hard disk), the USB device must be connected to the USB server port.

NOTICE: For more information on backing up data, see Immediate Backup .

Step by Step

1) Click on **Backup and Restore** in the navigation bar.
2) In the navigation tree, click **Backup - Immediate**.
3) Enter a comment for the backup set in the **Comment** field in the **Name** area so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) Activate the target drive on which the backup set is to be saved in the **Devices** area.
5) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.
6) The backup was successful if the message **Backup completed successfully!** appears. Click on **Finish**.
7) If you are using a USB stick as the backup medium, wait until the LED of the USB stick stops blinking. This ensures that the backup has been successfully saved on the USB stick. You can then safely remove the USB stick.
8) This completes the initial startup with WBM. Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

NOTICE: If a new software version for the communication system is available, you will be notified about this on the home page of the WBM, provided the Internet connection was set up correctly. If a new software version is available, perform an update (see Updating the Communication System).

5.9 Commissioning of IP Phones

The commissioning of IP phones can be facilitated by the existence of a DHCP server that supplies an IP phone with important (network-specific) data that is needed to log into the communication system.

Network-Specific Data

In order to log into the communication system, an IP phone requires some network-specific data. This data can be stored in the DHCP server or be entered directly at the IP phone. The advantage of a DHCP server is that all connected IP phones are automatically supplied with the relevant data.

The following data is required by the IP phone:

- IP address of the communication system
- IP address of DLS server

In addition, the IP phone needs its own call number. This must be entered manually when logging in at the phone.

Registration of SIP Phones

For security reasons, it is recommended that SIP phones register at the communication system. To do this, the registration information on the IP phone and the communication system must match.

The following data is required for the login:

- SIP user ID
- SIP password
- SIP realm (optional)

Use a non-trivial SIP password that complies with the following rules:

- At least 8 characters
- At least one uppercase letter (A - Z)
- At least one lowercase letter (a - z)
- At least one digit (0-9)
- At least one special character

Use a SIP user ID that does not include the phone number.

NOTICE: More information on configuring SIP telephones can be found at `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Using the Internal DHCP Server

If the internal DHCP server of the communication system is used, the network-specific data will already be stored there. In order to enable an IP phone to register at the communication system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server with Network-specific Data

If an external DHCP server is used, the network-specific data must be stored there. In order to enable an IP phone to register at the communication system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server without Network-specific Data

If an external DHCP server in which the network-specific data cannot be stored is used, this must be entered at the IP phone. To enable an IP phone to register at the communication system, the defined call number and IP address of the communication system must be entered at the phone, and the settings for the Deployment Service may need to be changed. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

5.9.1 How to Configure an IP Phone

Prerequisites

The IP phone is connected to the internal network and operational.

NOTICE: The sample configuration described here uses an OpenStage 40/60/80 IP system telephone. The same settings must also be made for any other IP phone. For more information, refer to the manual supplied with your IP phone.

Step by Step

1) To reach the administration mode of the IP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Admin` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the IP system telephone can be updated automatically. This applies only to IP system telephones. Proceed as follows:

a) Scroll to `Network` and confirm your selection with the OK key.
b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.
c) Scroll to `DLS address` and confirm your selection with the OK key.
d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.
e) Scroll to `Save & Exit` and confirm your selection with the OK key.
f) Scroll to `IPv4 configuration` and confirm your selection with the OK key.
g) Scroll to `Route (default)` and confirm your selection with the OK key.
h) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
i) Scroll to `Save & Exit` and confirm your selection with the OK key.
j) Navigate one menu level back with the Back key.

6) Specify the call number of the phone:

a) Scroll to `System` and confirm your selection with the OK key.
b) Scroll to `Identity` and confirm your selection with the OK key.
c) Scroll to `Terminal number` and confirm your selection with the OK key.
d) Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.
e) Scroll to `Save & Exit` and confirm your selection with the OK key.

7) Navigate one menu level back with the Back key.

8) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

5.9.2 How to Configure a SIP Phone

Prerequisites

The SIP phone is connected to the customer LAN and operational.

NOTICE: The configuration described here uses an OpenStage 40/60/80 SIP system telephone as an example. The same settings must also be made for another SIP phone. For more information, refer to the manual supplied with your SIP phone.

Step by Step

1) To reach the administration mode of the SIP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Administrator (Admin)` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the SIP system telephone can be updated automatically. This applies only to SIP system telephones. Proceed as follows:

a) Scroll to `Network` and confirm your selection with the OK key.
b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.
c) Scroll to `DLS address` and confirm your selection with the OK key.
d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.
e) Scroll to `Save & Exit` and confirm your selection with the OK key.
f) Scroll to `IPv4 configuration` and confirm your selection with the OK key.
g) Scroll to `Route (default)` and confirm your selection with the OK key.
h) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
i) Scroll to `Save & Exit` and confirm your selection with the OK key.
j) Navigate one menu level back with the Back key.

6) Specify the SNTP time settings:
   a) Scroll to `Date and time` and confirm your selection with the OK key.
   b) Scroll to `Time source` and confirm your selection with the OK key.
   c) Scroll to `SNTP IP address` and confirm your selection with the OK key.
   d) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
   e) Scroll to `Timezone offset` and confirm your selection with the OK key.
   f) Enter the deviation between the local time and UTC (Universal Time Coordinated) in hours (Germany: `1`) and confirm this with the OK button.
   g) Scroll to `Save & Exit` and confirm your selection with the OK key.
   h) Navigate one menu level back with the Back key.

7) Specify the call number of the phone:
   a) Scroll to `System` and confirm your selection with the OK key.
   b) Scroll to `Identity` and confirm your selection with the OK key.
   c) Scroll to `Terminal number` and confirm your selection with the OK key.
   d) Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.
   e) Scroll to `Save & Exit` and confirm your selection with the OK key.

8) Specify the SIP authentication data:
   a) Scroll to `Registration` and confirm your selection with the OK key.
   b) Scroll to `SIP Session` and confirm your selection with the OK key.
   c) Note the `Realm`, or enter a new realm (e.g., `OSBIZ-SIP`), if necessary.
   d) Note the `User ID`, or enter a new user ID (e.g., `SIP-120`), if necessary.
   e) Specify a `Password` for registering at the SIP server.
   f) Scroll to `Save & Exit` and confirm your selection with the OK key.

9) Use the Back key to go back to the `Admin` menu.

10) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

5.10 How to collect diagnostic traces for error incident

You can automatically collect the necessary diagnostic traces data for an error incident. 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.

Perform the following steps to collect the diagnostic trace data for the error incident:

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** next to **Error Management**.
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.

   For more information about the traces, see the Troubleshooting guide.
6) Click **OK & Next**.
7) A list with additional information, relevant documentation and hints is displayed. Click **OK & Next**.
8) The scenarios and type of traces that you will collect are displayed. Click **Finish**.
9) Continue by executing the problematic scenario.
10) Once you complete the scenario navigate again to **Setup > Error Management** and click **Edit**.

    You are redirected to the Step 2 of the diagnostic traces collection. If you want to stop the process and initiate it again you can click the **Abort** button.
11) Click **OK & Next**.
12) Enter the required information and click **OK & Next**.
13) A list with necessary information and some further actions is displayed.
14) Click **OK & Next**.
15) Click **Finish** to start downloading the diagnostic trace data.

5.11 Reflashing

Following the steps below you can easily change the software type of a device.

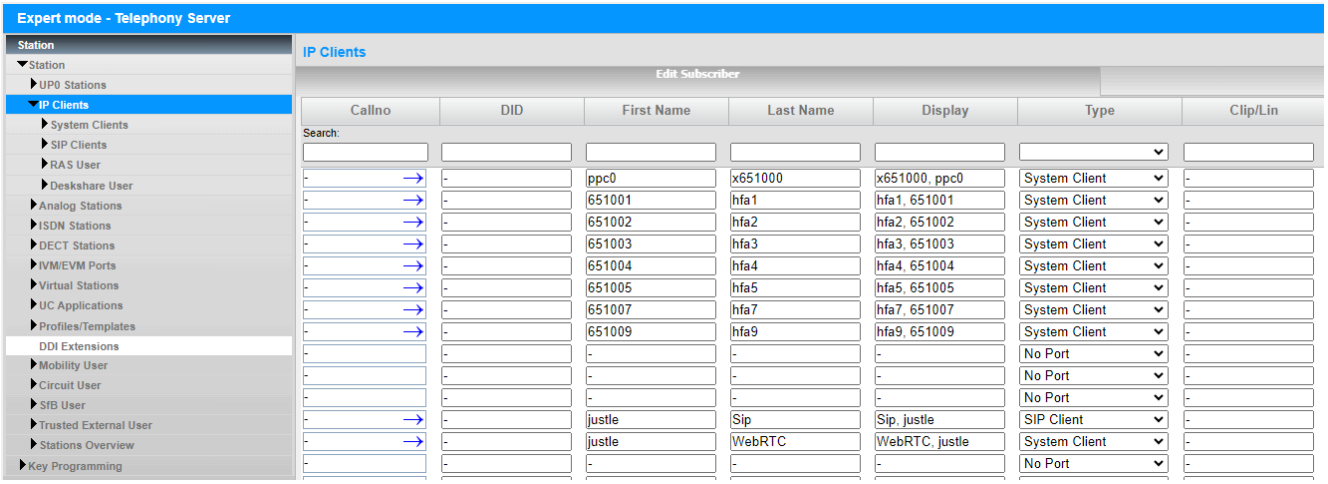
The concept behind this feature is to simplify the way of getting a SIP device (out of the box) and registering it to OSBiz system as an HFA device. The only requirements are:

- the phone must get the DLI address (either from DHCP server or manually)
- the administrator must enter the phone's number (which must be preconfigured as a System Client)

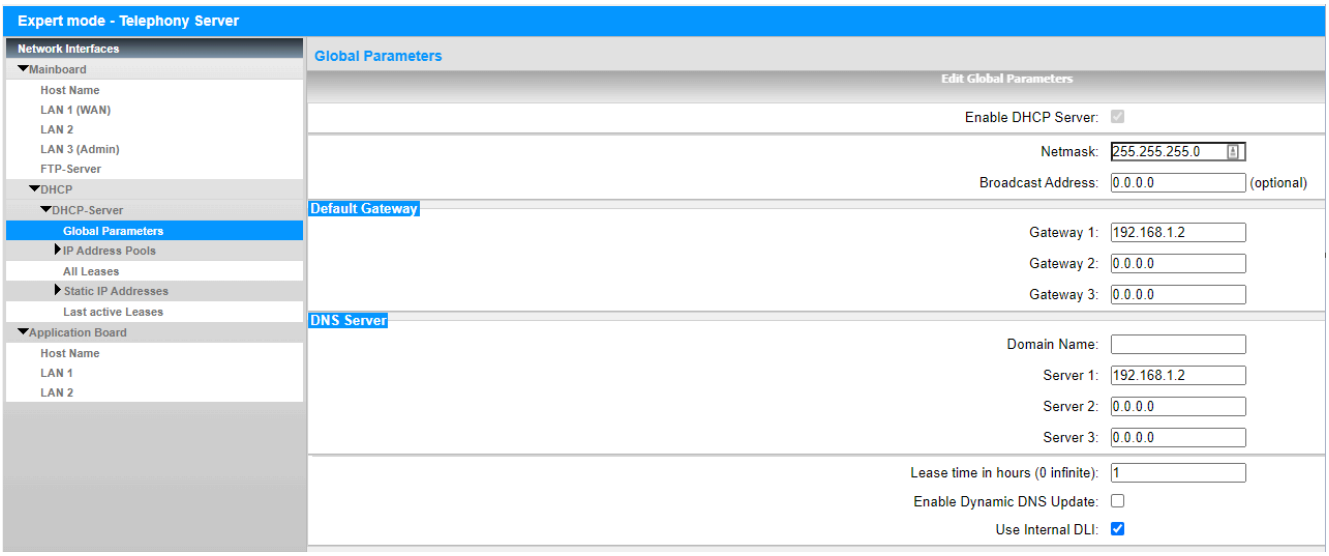
Once the customer gets a new device it will be pre-configured as a SIP device(factory settings). The steps to reflash this device to an HFA device are as follows:

Step by Step

1) Configure in the OSBIZ database the desired phone number as a System Client (HFA).



2) Configure the DHCP server to send the IP address of DLI. This can be done either at the external DHCP Server or the internal DHCP server.



3) If there is no DHCP server used, then you must configure the DLI IP on the phone manually.

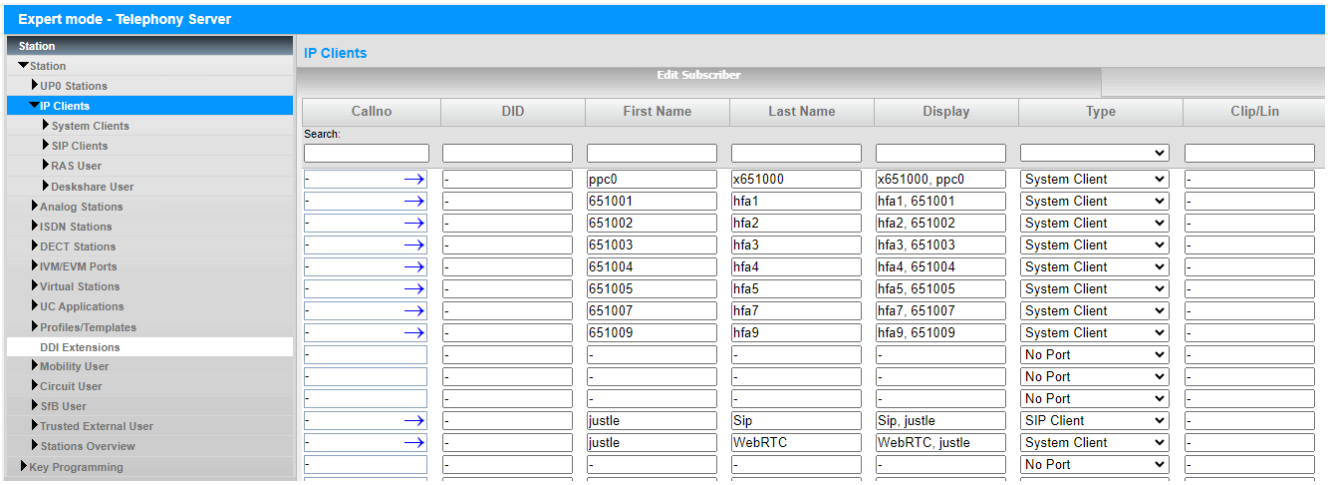
4) Once the SIP phone gets an IP and the DLI IP, the phone device will be registered into the DLI database, and a prompt will be displayed to enter the extension number.

5) Enter the terminal number on the phone (the number should be the same configured in the first step, e.g. 4111).

6) The reflash will start and the new HFA image will be downloaded to the phone. When the phone reboots it will be registered as an HFA phone and the plug and play data will be sent by the system towards the phone.

7) **To reflash an already registered SIP phone:**

8) Change the working SIP device to "System Client".



9) Restart the phone

10) The reflash will start and the new HFA image will be downloaded to the phone. When the phone reboots it will be registered as an HFA phone and the plug and play data will be sent by the system towards the phone.

6 Initial Setup for OpenScape Business S

The initial setup of OpenScape Business S (also referred to as the Softswitch in short) is described here. This includes the integrating the softswitch and related components into the existing customer LAN as well as setting up Internet access for Internet telephony and configuring the connected stations.

For OpenScape Business S, the OpenScape Business communication software is installed on the Linux operating system SLES 12 SP5 64 bit or SLES 15 SP6 64-bit. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere or Microsoft Hyper-V. The installation of the Linux operating system is described in the installation guide *OpenScape Business, Installing the Linux Server*.

The initial setup of OpenScape Business S is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM in short).

This section describes the configuration of the most common components. Not all of these components may be used by you. During the initial setup, you may need to choose between multiple options in some places or even skip some configurations entirely, depending on which components you use.

The detailed administration of any features that are not covered by the initial setup is described in subsequent chapters.

The initial setup requires the creation of an IP address scheme and a dial plan.

Summary of the most important installation steps:

- System settings
- System Phone Numbers and Networking
- Internet Telephony
- Station configuration
- Licensing
- System hardening
- Data backup

6.1 Prerequisites for the Initial Setup

Meeting the prerequisites for the initial setup ensures the proper operation of OpenScape Business S.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.
- The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- All licenses required for OpenScape Business S are present (e.g., UC clients, Directory Services, etc.).
- An IP address scheme exists and is known.

- A dial plan (also called a numbering plan) is present and known.

Software

The following software is required for the installation of OpenScape Business S:

- DVD or .ISO image with the OpenScape Business communication software

  Contains the OpenScape Business communication software. This DVD or .ISO image is included in the delivery package.
- DVD or USB stick with Linux operating system SLES 12 SP5 or SLES 15 SP6.

  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD or .ISO image.

Administration

For the initial setup of OpenScape Business S with the OpenScape Business Assistant (WBM), the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system.

- Web browsers:

  The following HTML 5-enabled web browsers are supported:

  – Microsoft Internet Explorer Version 11 and later (Admin PC).
  – Microsoft Edge
  – Mozilla Firefox Version 37.x and 38.x
  – Mozilla Firefox ESR Version 24.x and 31.x
  – Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Java:

  Oracle Java 8 or higher or alternatively OpenJDK 8 must be installed. If an older version is installed, you will need to update it to the latest version before you can start setting up the system for the first time.

- Screen resolution: 1024x768 or higher

Firewall

When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see Used Ports).

Internet Access

The Server PC must have broadband Internet access for:

- Security patches and general Linux software updates

OpenScape Business requires an Internet connection for:

- OpenScape Business software updates
- OpenScape Business features such as Internet telephony, for example
- OpenScape Business Mobility Clients such as myPortal to go, for example
- Remote Service

E-mail Server (Optional)

OpenScape Business requires access to an e-mail server in order to send e-mails. For this purpose, the access data to the E-mail server must be entered in OpenScape Business, and the relevant accounts (IP address, URL, login data of the E-mail server) must be set up in the E-mail server.

If the e-mail functionality is not used within OpenScape Business, this data need not be entered.

Internet Telephony, VoIP (Optional)

If Internet telephony is used within OpenScape Business, then OpenScape Business will require broadband access to the Internet and to an Internet Telephony Service Provider (ITSP, SIP Provider) for SIP telephony over the Internet. To do this, the appropriate accounts must be obtained from the ITSP, and the access data for the ITSP (IP address, URL, login data of the SIP Provider) must be set up in OpenScape Business.

Second LAN Port

If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs. The configuration of Internet access occurs in the external Internet router of the customer LAN. The setup of the second LAN port occurs directly during the initial setup of Linux or can be performed later using YaST. In the WBM, the second LAN port only needs to be activated as a WAN interface.

Fax as PDF

If faxes are to be saved in PDF format, the server PC requires at least 4 GB RAM. If OpenScape Business S is being operated in a virtual environment, the virtual machine must also be assigned 4GB RAM.

6.2 Components

The various components of the installation example are described and outlined below.

The installation example includes the following components:

- OpenScape Business S

  The Linux server with the OpenScape Business S communication software is integrated in the existing customer LAN via its LAN interface.
- Admin PC

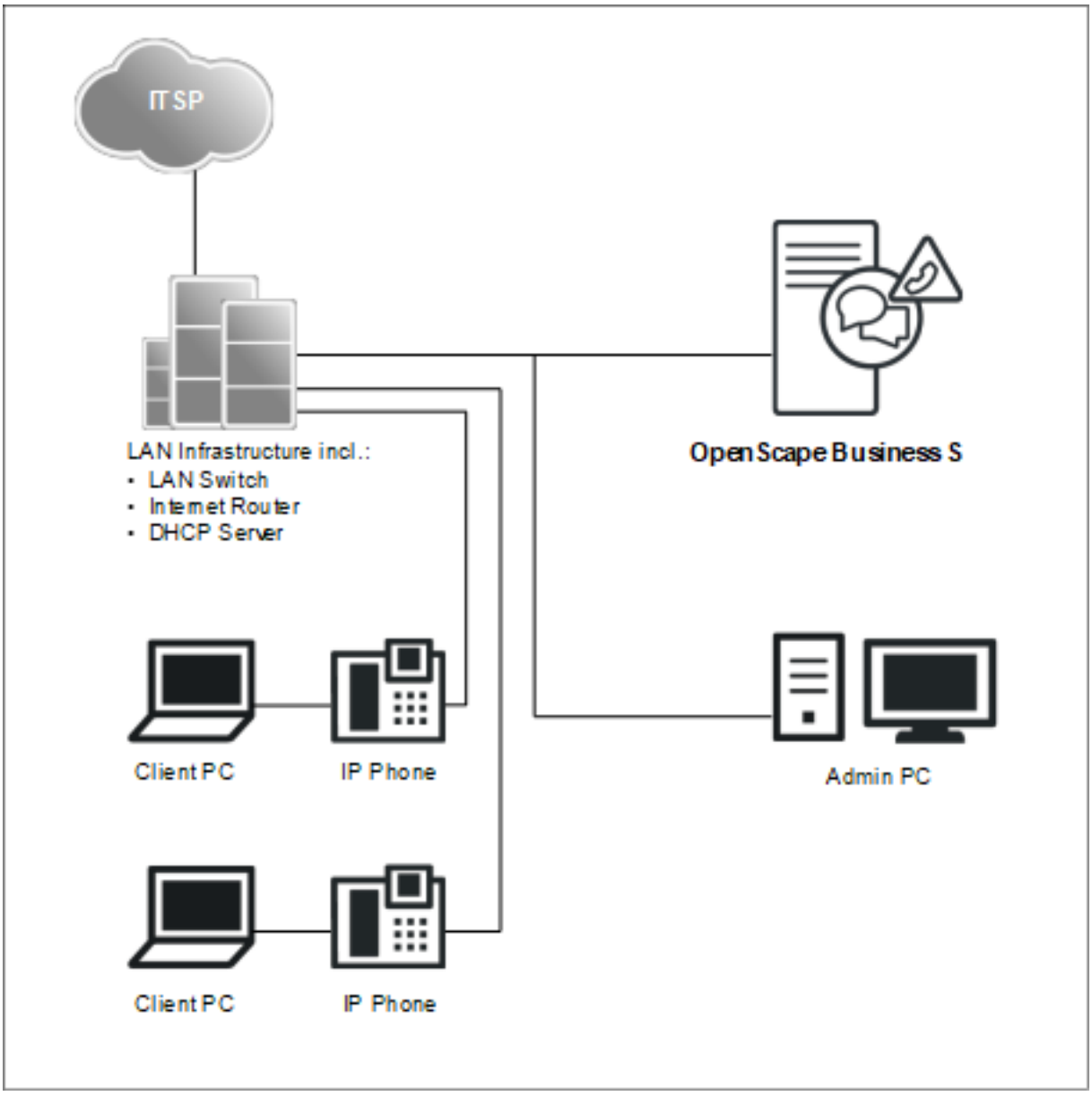
  The admin PC is also integrated in the existing customer LAN via its LAN interface.

- IP stations (IP clients)

  The IP stations (IP system phones, client PCs, WLAN Access Points, etc.) are integrated in the LAN via one or more switches.

The IP clients obtain their IP addresses dynamically from an internal DHCP server (DHCP server of the Linux server) or from an external DHCP server (DHCP server of the Internet router, for example).

Internet access is configured in the Internet router.



6.3 IP Address Scheme

An IP address scheme is a definition of how the IP addresses are used in the customer LAN. It includes the IP addresses of PCs, servers, Internet routers, IP phones, etc.

To provide a better overview of the assignment of IP addresses, an IP address scheme should be created.

Example of an IP address scheme with the IP address range `192.168.5.x`:

IP address range	Clients
192.168.5.1 through **192.168.5.49**	Clients with a fixed IP address
192.168.5.1	Internet router (gateway)
192.168.5.10	Server PC (OpenScape Business S)
192.168.5.20	E-mail server
192.168.5.100 to **192.168.5.254**	Client PCs & IP phones, also the IP address range of the DHCP server; IP addresses are assigned automatically to the clients

6.4 Dial Plan

A dial plan is a list of all phone numbers available in the communication system. It comprises internal phone numbers, DID numbers, and group station numbers.

Default Dial Plan

The internal call numbers are preassigned default values. These values can be adapted to suit individual requirements as needed (e.g., to create individual dial plans).

Extract from the default dial plan:

Type of call numbers	Default call numbers
Internal station numbers	100-349, 500-709
User direct inward dialing numbers	100-349, 500-709
Group station numbers	350-439
Voicemail call number	71
Announcement Player call number	72
Seizure codes (external codes): Central Office ITSP	855-858
Call number for conferences	7400-7404
Call number for parking	7405
Call number for AutoAttendant	7410-7429
Call number for MeetMe conference	7430

Individual Dial Plan

An individual dial plan can be imported in the WBM via an XML file during the basic configuration.

The XML file contains several tabs. Besides the names and phone numbers of subscribers, the "Customer" tab also includes additional subscriber data such as the subscriber types and e-mail addresses of the subscribers.

A sample XML file with the appropriate explanations can be found in the WBM under **Service Center** > **Documents** > **Templates** > **CSV Templates**. You can also use the XML file stored there as a template for your data. It can be edited with Microsoft Excel, for example.

6.5 Installing the Communication Software

The OpenScape Business S communication software is installed on the Linux server.

Make sure that the IP addresses and network masks to be configured are appropriate for the customer LAN.

DHCP Server

A DHCP server automatically assigns a unique IP address to each IP station (IP phones, PCs, etc.) and provides the IP stations with network-specific data such as the IP address of the default gateway, for example.

Either an external DHCP server (e.g., the DHCP server of the Internet router or of the communication system) or the DHCP server of the Linux server can be used as a DHCP server. If the DHCP server of the Linux server is used, the external DHCP server must be disabled. The configuration of the Linux DHCP server can be performed during the installation of the OpenScape Business communication software.

NOTICE: You should active DHCP either from yast or from WBM, but not from both. If you activate the DHCP during the initial installation of OpenScape Business S, it is equivalent to activating the DHCP through yast. If you want to activate DHCP on OpenScape Business S from WBM, then the DHCP should not be activated during the initial installation of the communication software.

Virtual Environment

The communication software can run in a virtual environment. There are two ways to perform the installation:

- Separate installation of Linux and the communication software

  To do this, the virtualization software (host operating system) must be first installed and configured on the server PC. Linux is installed in the virtual environment as a guest operating system. Within the Linux operating system, the communication software is installed last with the help of the OpenScape Business DVD or .ISO file (see *OpenScape Business Linux Server, Installation Guide* for more details).
- Combined installation of Linux and the communication software (VMWare only)

  To do this, the virtualization software (host operating system) must be first installed and configured on the server PC. An OVA image (Open Virtualization Appliance), which includes Linux and the communication

software, is installed in the virtual environment. The OVA image is provided through the software supply server (SWS).

For more than 50 users, the home partition must be resized after the installation to 100 GB (for 50 to 100 users) or 200 GB (for up to 500 users or for OpenScape Business Contact Center) or 500 GB (for more than 500 users).

For Linux updates, you will also need the OpenScape Business SLES upgrade key in order to be able to register with Linux.

Use of snapshots on virtual machines (VM):

Snapshots can be a valuable maintenance mechanism, for example, to perform a fast rollback to a predefined operating state of the VM after a mass distribution script has failed.

- Snapshots cannot be created during normal operation. The current operating state of the virtual machine is frozen while taking a snapshot. Consequently, connected terminals and applications such as IP phones or the UC clients may lose the connection to the server.
- Snapshots can cause internal server processes to lose their synchronization, which means that the stable operation of the communication system can then no longer be guaranteed. A server reboot following the snapshot should therefore also be planned within the maintenance timeframe.
- Previous snapshots should not remain on the production environment during normal operation.
- Snapshots can be taken during a planned maintenance window or within the framework of the installation.
- Snapshots are used internally by backup tools such as VDP or VDR. It must be ensured that these backup operations are schedules outside of business hours and that the snapshots generated by these tools are deleted at the end of the operation.

More information regarding snapshots can be found in the VMware knowledge base (KB). A good starting point is the KB article 1025279 – Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

All information about snapshots in Microsoft Hyper-V can be found in the technet library at technet.microsoft.com within the Hyper-V chapter.

6.5.1 How to Install the Communication Software

Prerequisites

- The SLES 12 SP5 or SLES 15 SP6 operating system has been correctly installed and started on the Linux server.
- DVD or .ISO file with OpenScape Business communication software.
- DVD or .ISO file or USB stick with the Linux operating system SLES 12 SP5 64-bit or SLES 15 SP6 64-bit, for any subsequent installation of software packages (RPM) that may be required.
- The root access data (user name and password) for logging into the Linux server is available.

IMPORTANT: The OpenScape Business communication software overwrites any existing configuration files (e.g., for DHCP, FTP, Postfix, etc.) during the installation.

Step by Step

1) Log into the Linux server with root privileges.
2) Insert the OpenScape Business DVD or .ISO file into the DVD drive.
3) Confirm the message with **Run**. The "Welcome" window appears.
4) Select the desired setup language (e.g., **English**) and click **Start**. The rest of the installation is described here for the English language.
5) Select the desired product from the list and click on **Select**. A check is performed to determine whether the hardware meets all the requirements for the installation. A warning is displayed for minor shortfalls in meeting the requirements. After confirmation, the installation can then be continued. For severe shortfalls, the installation is canceled automatically.
6) A check is performed to determine whether additional RPM packages need to be installed. If yes, confirm this with **Confirm**. If this occurs, you will need to switch back to SLES 12 or SLES 15, DVD or .ISO file later.
7) A window with the terms of the license (i.e., the End User License Agreement or EULA) appears. Read the terms of the license and accept the license agreement with **Yes**.
8) If a DHCP server is already present in the customer LAN (e.g., the DHCP server of the Internet router), stop the configuration of the Linux DHCP server here with **No** and proceed to step 12 to continue.

   NOTICE: In order to ensure that the software of system telephones can be updated automatically even when using an external DHCP server, you have two options:

   a) The IP address of the Linux server must be entered as the DLS address at each system telephone.

   b) The network-specific data must be entered at the external DHCP server. The parameters for this can be found under `/var/log/OPTI.txt`.

9) If you want to use the Linux DHCP server, click on **Yes** to enable and configure the Linux DHCP server.
10) Enter the following values (preset with default values):
    - **Default Route**: IP address of the default gateway; as a rule, the IP address for the Internet router, e.g., `192.168.5.1`.
    - **Domain** (optional): the domain specified during the Linux installation, e.g., `<customer>.com`
    - **DNS-Server** (optional): IP address of the DNS server specified during the Linux installation. If no DNS server is available in the internal

network, you can enter the IP address of the Internet router (e.g., `192.168.5.1`) here.
- **SNTP Server**: IP address of the internal or external NTP server.
- **DLS/DLI Server**: IP address of DLS server, i.e., the IP address of the Linux server (e.g.: `192.168.5.10`).
- **Subnet**: appropriate subnet for the IP address range, e.g.: `192.168.5.0`.
- **Netmask**: Subnet mask of the Linux server that was specified during the Linux installation, e.g.: `255.255.255.0`.
- **IP range begin** and **IP range end**: IP address range from which the DHCP server may assign IP addresses, e.g.: `192.168.5.100` to `192.168.5.254`.

11) Click on **Continue**.

12) After the installation, the Linux operating system needs to be restarted. Select the check box **PC Reboot** and confirm with **Continue**.

13) If additional RPM packages need to be installed, you will be prompted to insert the SLES 12 DVD or SLES 15 USB stick. Insert the DVD or USB stick and confirm with **Continue**. Following the successful installation of the RPM packages, reinsert the OpenScape Business DVD or .ISO file and confirm this with **Continue**, followed by **Run**.

14) The OpenScape Business communication software is installed. The operating system then automatically performs a restart.

15) After the restart, log in with the user account that was set up earlier during the Linux installation.

16) Right-click on the DVD drive icon on the desktop and select the menu item **Eject**. Remove the OpenScape Business DVD from the DVD drive.

NOTICE: It takes a few minutes until all components of the OpenScape Business communication software are active.

6.6 Starting Up

The basic settings are made using the **Initial Installation** wizard of the WBM.

6.6.1 How to Start the Initial Installation Wizard

Prerequisites

The WBM has been started.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click on **Edit** to start the **Initial Installation** wizard.

NOTICE: If the size of the browser window cannot display the workspace in its entirety at low screen resolutions, a horizontal or vertical scroll bar appears at the sides and can be used to scroll to the required section.

Next steps

Perform initial installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

6.6.2 System Settings

The **System Settings** window is used to configure the system settings of the communication system.

Proceed as follows:

1) Set the display logo and the product name

Specify a display text to be displayed on the display of the system phones. Additionally, you can also select the product name.

2) Select the country code and the language to be used for event logs

For country initialization to work correctly, you must select the country in which the communication system is operated. In addition, you can select the language in which the event logs (system event logs, errors logs, etc.) are to be stored.

3) Only if required: Activate another LAN port as a WAN interface

If OpenScape Business S (or the Linux server) has a second LAN port, you can use this as a WAN interface for Internet access and Internet telephony via an ITSP. The first LAN port is used as usual as a LAN interface for the internal phones and PCs.

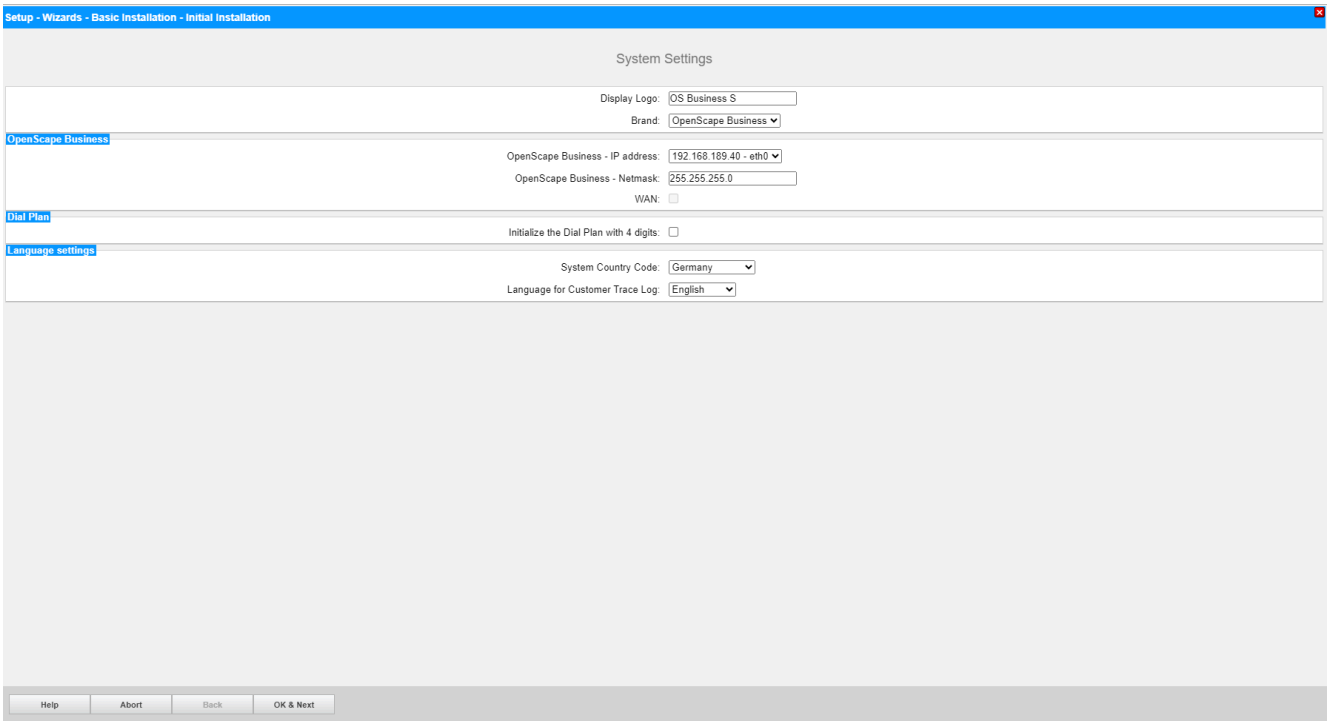
4) Change the default dial plan to 4 digit numbers (available only for OSBiz S)

In a fresh system installation you can initialize the dial plan with 4 digits, instead of 3. Doing so changes the system's default numbers from 100, 101, 102, ..., to 1000, 1001, 1002, and so on. This allows the automatic call number allocation for a high number of user stations. Note that after enabling this flag, the system restarts.

6.6.2.1 How to Set the Display Logo and Product Name

Prerequisites

You are in the **System Settings** window.



Step by Step

1) In the **Display Logo** field, enter a text of your choice (e.g., OS Business S). The text can contain up to 16 characters. Avoid the use of diacritical characters such as umlauts and special characters.
2) Select the desired product name in the **Brand** drop-down list.

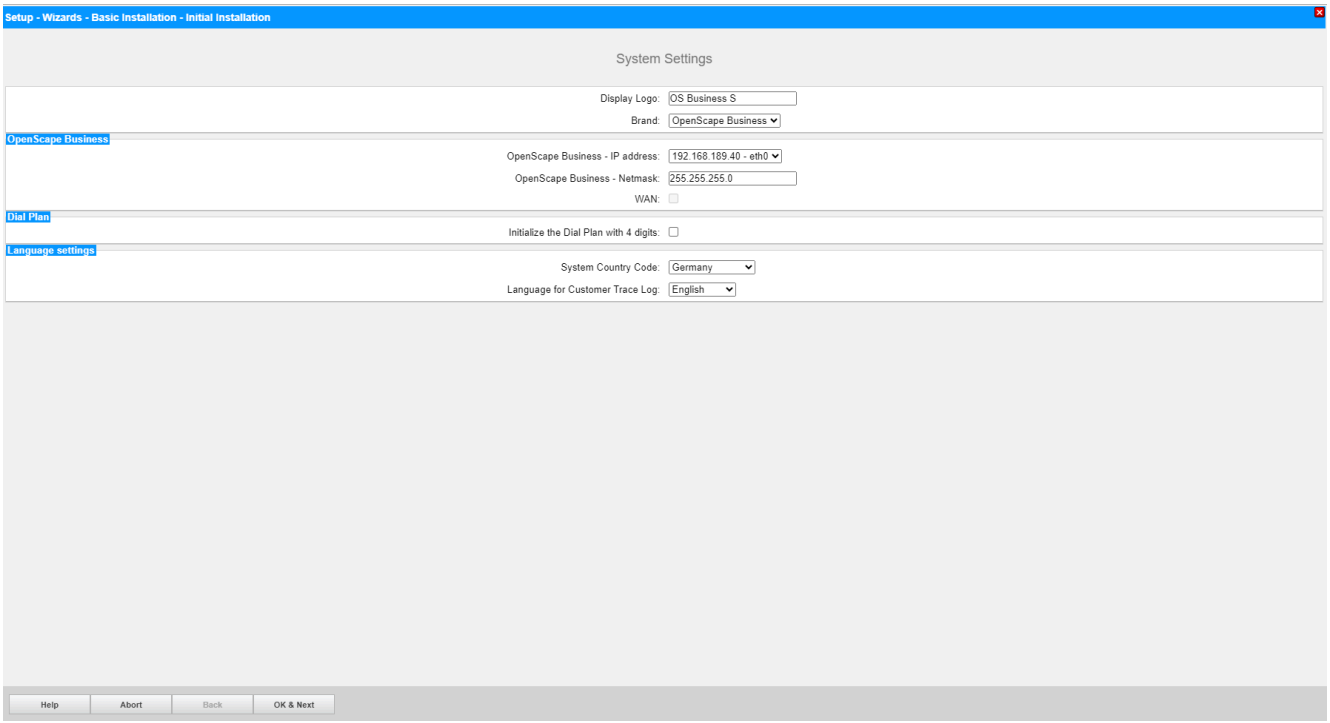
Next steps

Select the country code and language to be used for the trace logs.

6.6.2.2 How to Select the Country Code and the Language for Trace Logs

Prerequisites

You are in the **System Settings** window.



Step by Step

1) In the **System Country Code** drop-down list, select the country where the communication system is operated.
2) In the **Language for Customer Trace Log** field, enter the language in which the event logs (system event logs, error logs, etc.) are to be output.

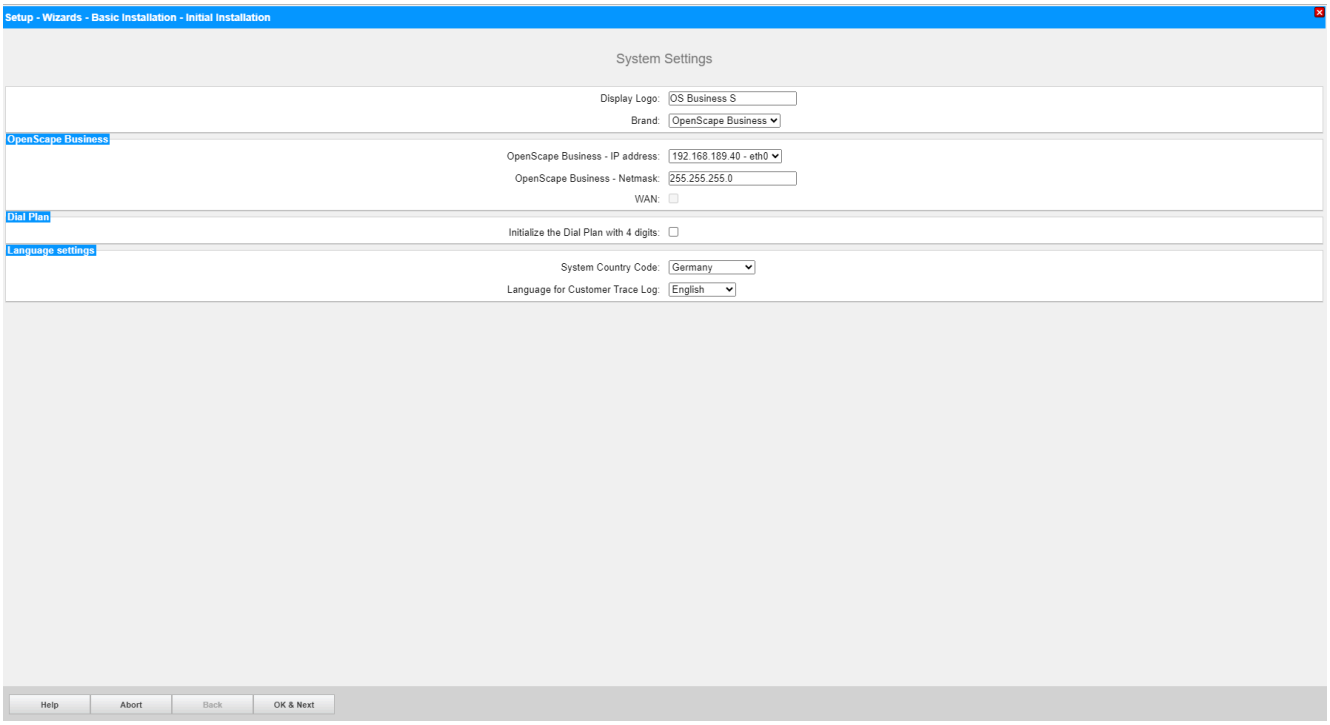
Next steps

Start the basic configuration.

6.6.2.3 How to Activate an Additional LAN Port as a WAN Interface

Prerequisites

You are in the **System Settings** window.



Step by Step

1) Select the **WAN** check box.
2) Select the desired LAN port (e.g., `eth1` or `eth2`) from the **OpenScape Business - IP Address (WAN)** drop-down list. If only two LAN ports are available, the second LAN port `eth1`is activated automatically.

> **NOTICE:** The assignment of IP addresses and subnet masks to the LAN ports is done during the initial installation of Linux or subsequently via YaST.

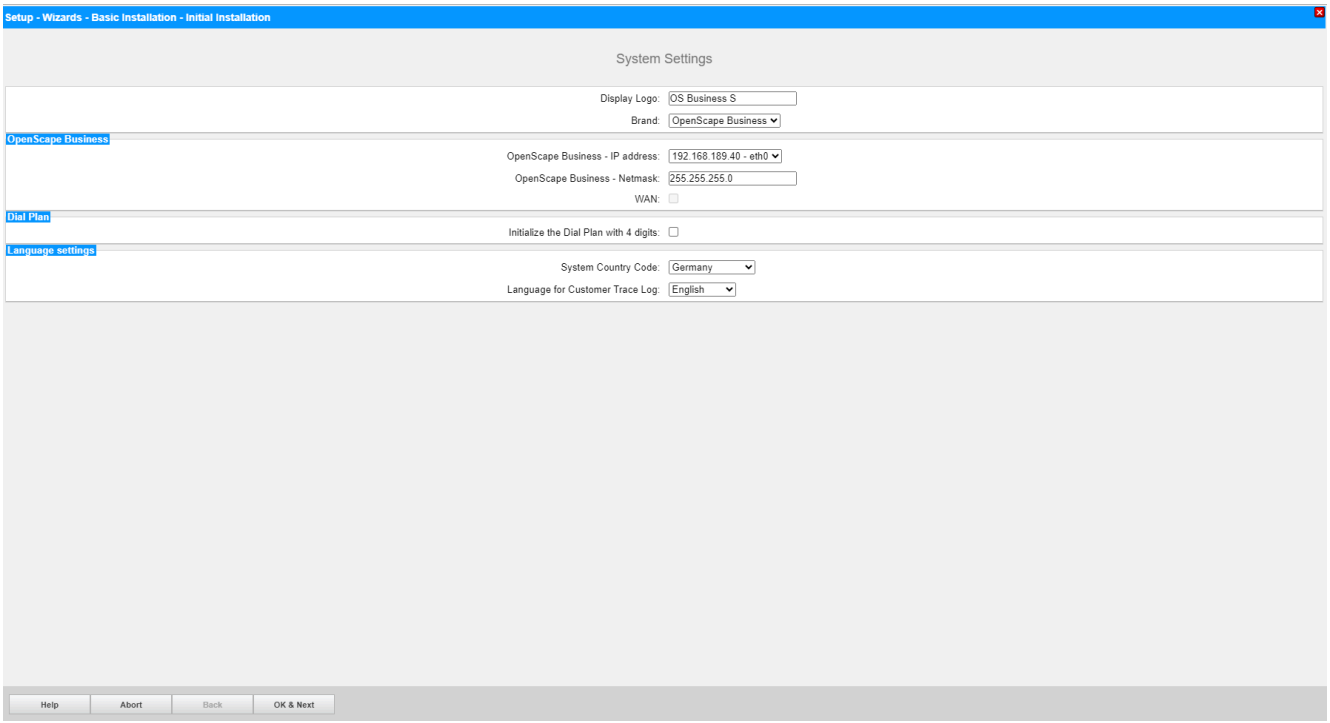
Next steps

Specify UC solution.

6.6.2.4 How to Change the Dial Plan to 4 Digits

Prerequisites

You are in the **System Settings** window.



Step by Step

Click on the check-box of the **Initialize the Dial Plan with 4 digits** field.

Next steps

System restarts

6.6.3 UC Solution

In the **Change application selection** window, select the UC solution to be used.

You have the following options:

- **Package with UC Smart**

  The UC solution UC Smart is integrated in OpenScape Business S.
- **Package with UC Suite**

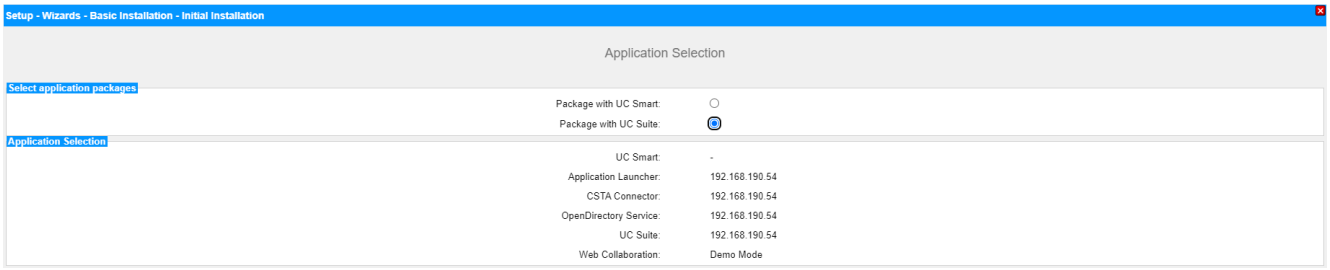
  The UC solution UC Suite is integrated in OpenScape Business S.

6.6.3.1 How to Define the UC Solution

Prerequisites

You have purchased licenses for either of the UC solutions, UC Smart or UC Suite.

You are in the **Application Selection** window.



Step by Step

1) If you use the UC solution UC Smart, click **Package with UC Smart**.
2) If you are using the UC solution UC Suite, click on **Package with UC Suite**.
3) Click on **OK & Next**.
4) The **Initial installation** wizard is closed. Click on **Finish**.

Next steps

Start the basic configuration.

6.7 Basic Configuration

The **Basic Installation** wizard is used for basic configuration. Basic configuration includes the most important settings for operating the communication system.

The Basic Installation Wizard includes a progress indicator showing the current step, as well as the steps that follow.

6.7.1 How to Start the Basic Installation Wizard

Prerequisites

The **Initial installation** has been completed.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Basic Installation** wizard.

Next steps

Perform basic installation as described in the following step-by-step instructions. Fields that are not described here are preset for the default scenario and should only be changed if they are not appropriate for your network data. For detailed information, refer to the descriptions provided in the Administrator documentation for the individual wizards.

6.7.2 System Phone Numbers and Networking

Enter the system phone numbers (PABX number, country and area code, international prefix) in the **Overview** window and specify whether OpenScape Business is to be networked with other OpenScape Business systems.

Proceed as follows:

1) Enter system phone numbers

- Enter system phone numbers for point-to-point connection

  Here you enter the system phone number for your point-to-point connection and the country code and area code.

  The entry of the country code is mandatory for Internet telephony and conference server functionality.

  The international prefix is preset, depending on the previously dialed country code.
- Enter system phone numbers for point-to-multipoint connection

  Here you enter the country code and area code for your point-to-multipoint connection.

  The entry of the country code is mandatory for Internet telephony and Meet-Me conferences.

  The international prefix is preset, depending on the previously dialed country code.

2) Activate or deactivate networking

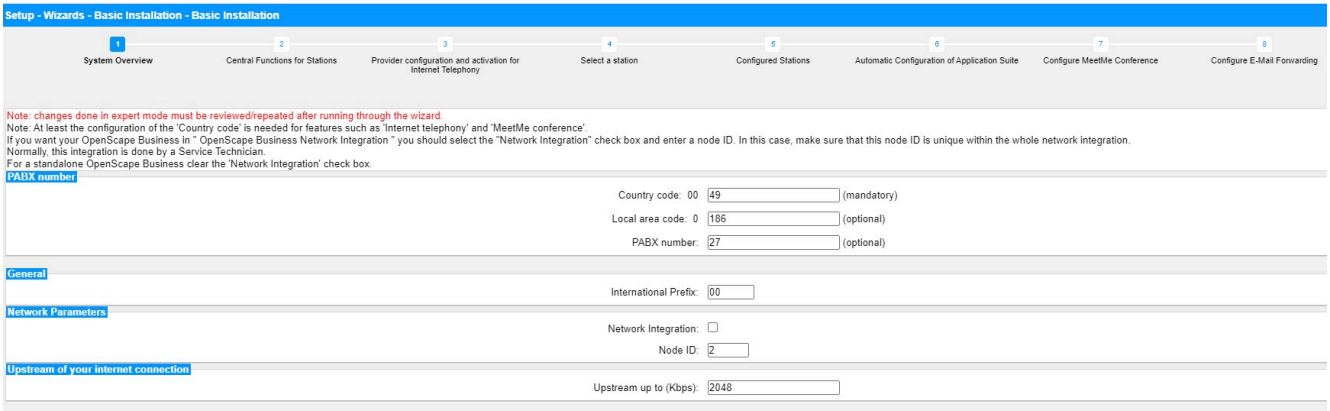
If OpenScape Business is to be networked with other OpenScape Business systems, networking must be enabled, and OpenScape Business must be assigned a node ID. Every OpenScape Business must have a unique node ID in the network.

6.7.2.1 How to Enter the System Phone Numbers for a Point-to-Point connection

Prerequisites

You have a point-to-point connection.

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.
3) Enter the system phone number of your trunk connection, e.g., `7007` (your connection number), in the **PABX number** field.
4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

Next steps

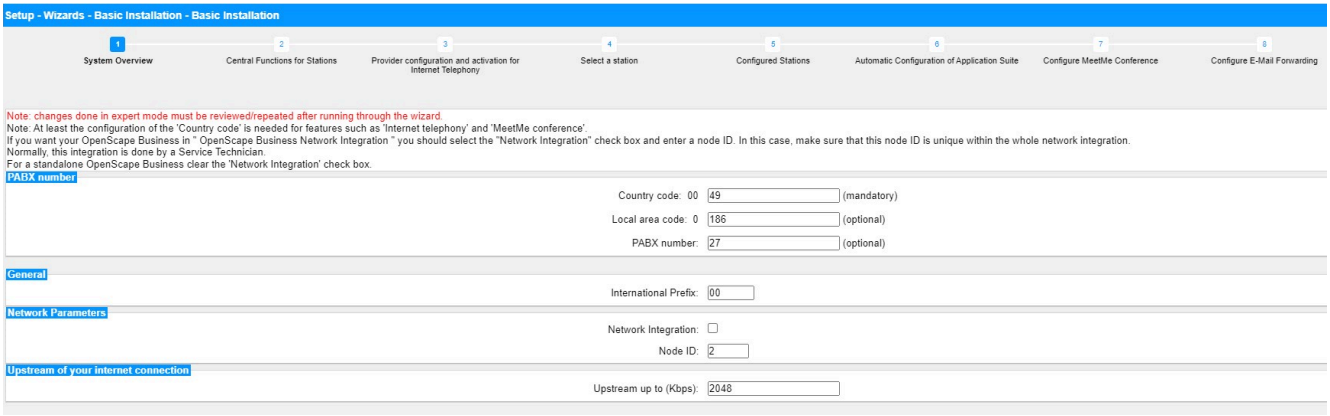
Activate or deactivate networking

6.7.2.2 How to Enter the System Phone Numbers for a Point-to-Multipoint Connection

Prerequisites

You have a point-to-multipoint connection.

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
2) Enter the local area code, e.g., `89` for Munich, in the **Local area code** field.
3) Leave the **PABX number** field empty.
4) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., "00-1-..." for calls from Germany to the USA and "011-49-..." for calls from the USA to Germany.

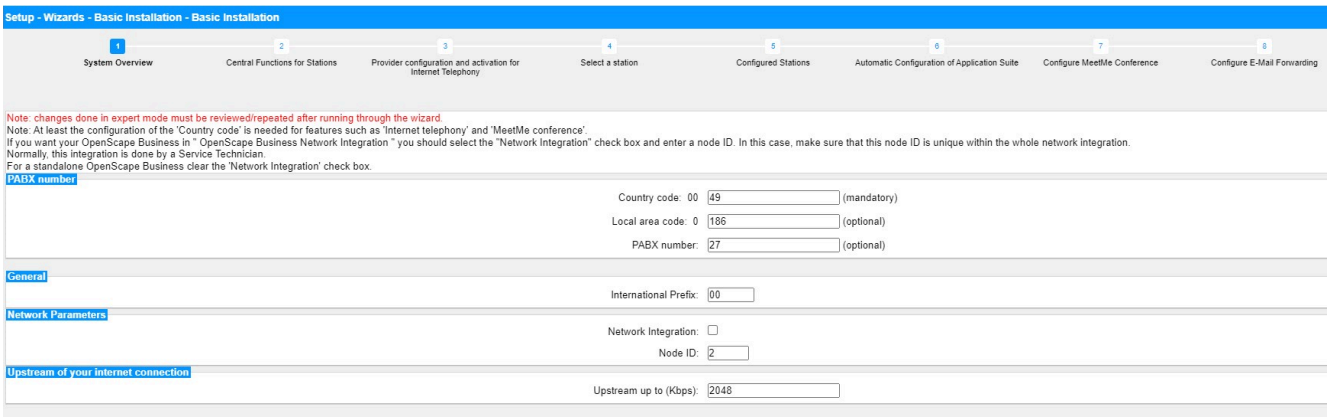
Next steps

Activate or deactivate networking

6.7.2.3 How to Activate or Deactivate Networking

Prerequisites

You are in the **System Overview** window of the **Basic Installation** wizard.



Step by Step

1) If the communication system is to be networked with other communication systems:
   a) Select the **Network Integration** check box.
   b) In the **Node ID** field for the communication system, enter a node ID that is unique in the internetwork (digits from `1` through `100` are possible).
2) If the communication system is not to be networked with other communication systems, leave the **Network Integration** check box disabled.

Next steps

Configure the upstream of your Internet connection.

6.7.2.4 How to Configure the Upstream of your Internet connection

Prerequisites

You are in the **Summary** window.

Step by Step

1) In the **Upstream up to (Kbps)** field, enter the speed of your Internet connection.
2) Click on **OK & Next**.

Next steps

Configure the station data.

6.7.3 Station Data

If necessary, you can configure your own individual dial plan instead of the predefined default dial plan in the **Central Functions for Stations** window and

import additional station data. In an internetwork, the default dial plan must be adapted to the dial plan of the internetwork.

The default dial plan contains predefined numbers for different types of stations (IP phones, analog phones, ...) and for special functions (Internet telephony, voicemail box, AutoAttendant, ...).

The station data includes the internal call numbers, DID numbers and names of the stations. This data and other station data can be imported into the communication system during the basic configuration via an XML file in UTF-8 format.

NOTICE: An XML template with the appropriate explanations can be found in the WBM under **Service Center** > **Documents** > **CSV Templates**. You can enter your data in this template by using Microsoft Excel, for example.

You have the following options:

- **Configure station data without an internetwork**

  Proceed as follows:

  1) Display the station data

  You can have all preconfigured station numbers and station data displayed.

  2) Delete all station numbers (optional)

  If you use an individual dial plan, you must delete all preconfigured station numbers.

  3) Adapt preconfigured station numbers for the individual dial plan (optional)

  If you are using an individual dial plan, you can adapt the preconfigured phone numbers to your own dial plan.

  NOTICE: If the user passes through the **Change preconfigured functional call numbers,** any existing custom configuration done in UC Suite must be reviewed or repeated (e.g., pilot queues)

  ---

  4) Import station data from an XML file (optional)

  You can easily import your individual station numbers, including any additional station data, during the basic configuration via an XML file.

- **Configure station data with an internetwork**

  Proceed as follows:

  1) Delete all station numbers

  If the UC Suite is used in an internetwork, a closed numbering plan is required, i.e., all station numbers in the internetwork must be unique. For this reason, any preconfigured station numbers must be deleted and only stations numbers adapted for the internetwork must be used.

  2) Import station data from an XML file

  The station numbers adapted for the internetwork and any additional station data can be easily imported during the basic configuration via an XML file. This file can contain all stations in the internetwork. During

import, only the station numbers and the station data assigned to the previously specified node ID of the communication system will be transferred.

Related tasks

How to display Mass data on page 156
How to Reset the LCR Entries on page 1345

Related reference

LCR > LCR flags on page 1533

6.7.3.1 How to Display the Station Data

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Select the **Display stations configuration** radio button.
2) Click on **Execute function**. A list of stations with the preconfigured phone numbers (default dial plan) is displayed.
3) Click on **OK**. You are taken back to the **Central Functions for Stations** window.
4) If you do not want to change any station data, click **OK & Next**.

6.7.3.2 How to Delete all Call Numbers

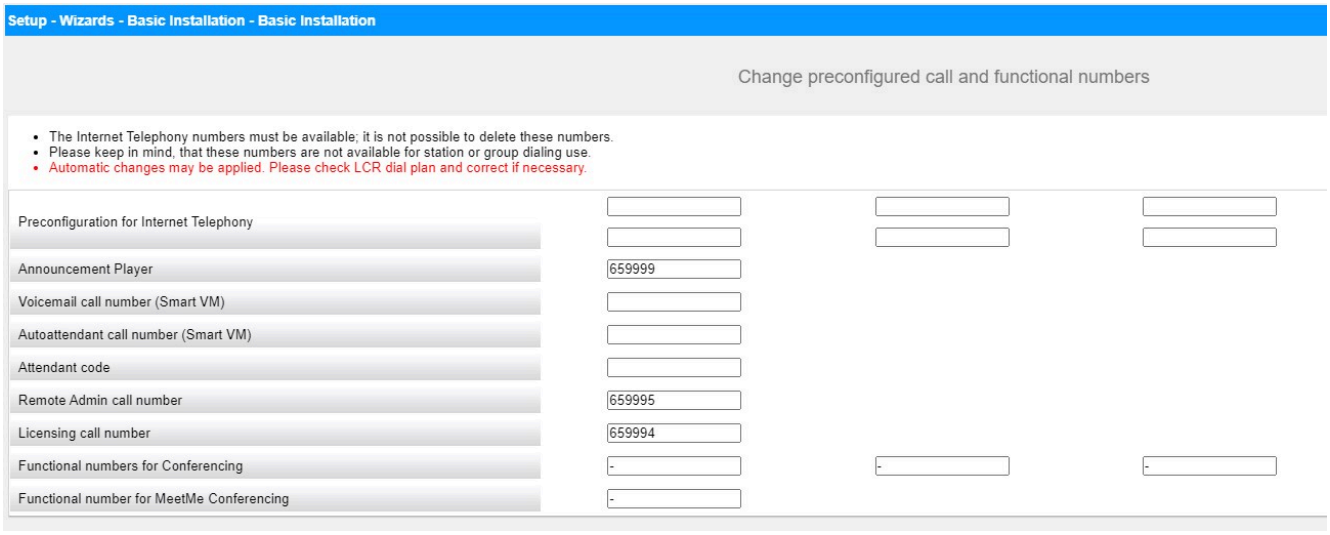
Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Enable the radio button **Delete all station call numbers**.
2) Enable the check box **Delete All Call Addresses**.
3) Click on **Execute function**. All preset call numbers are deleted except **Announcement Player, Remote Admin call number** and **Licensing call**

number. The **Change preconfigured call and functional numbers** window then appears.



4) Adjust the codes and special call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.
5) If you do not want to change any further station data, click **OK & Next**.

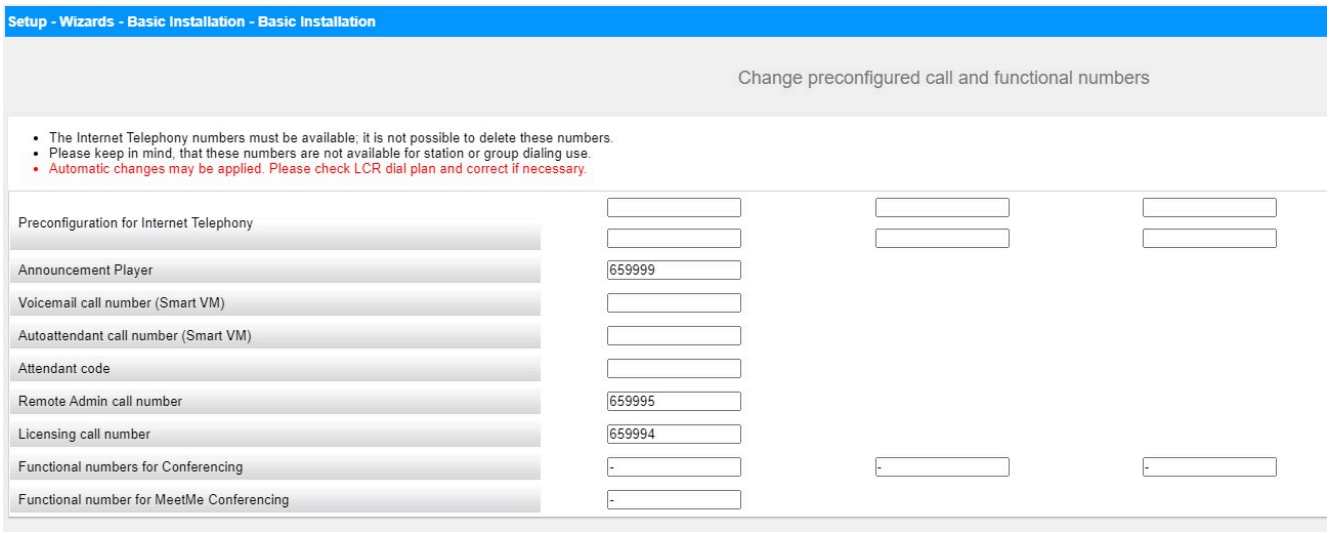
6.7.3.3 How to Adapt Preconfigured Station Numbers for the Individual Dial Plan

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

Step by Step

1) Enable the radio button **Change preconfigured call and functional numbers**.
2) Click on **Execute function**. The **Change preconfigured call and functional numbers** window appears.



3) Adjust the preconfigured call numbers to suit your preferences, and then click **OK**. You are taken back to the **Central Functions for Stations** window.
4) If you do not want to change any further station data, click **OK & Next**.

6.7.3.4 How to Import the Station Data from an XML File

Prerequisites

You are in the **Central Functions for Stations** window of the **Basic Installation** wizard.

An XML file with the entered data is available in UTF-8 format. An XML template can be found under **Service Center** > **Documents** > **CSV Templates**.

Step by Step

1) Enable the radio button **Import CSV/XML file with station data**.
2) Click **Execute function**.
3) Use **Browse** to select the created XML file and click **Open**.
4) Click **OK** when finished. The station data is imported.
5) Click **OK & Next**.

6.7.4 Internet Access

6.7.4.1 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP

Prerequisites

You have created a new network interface in the SLES.

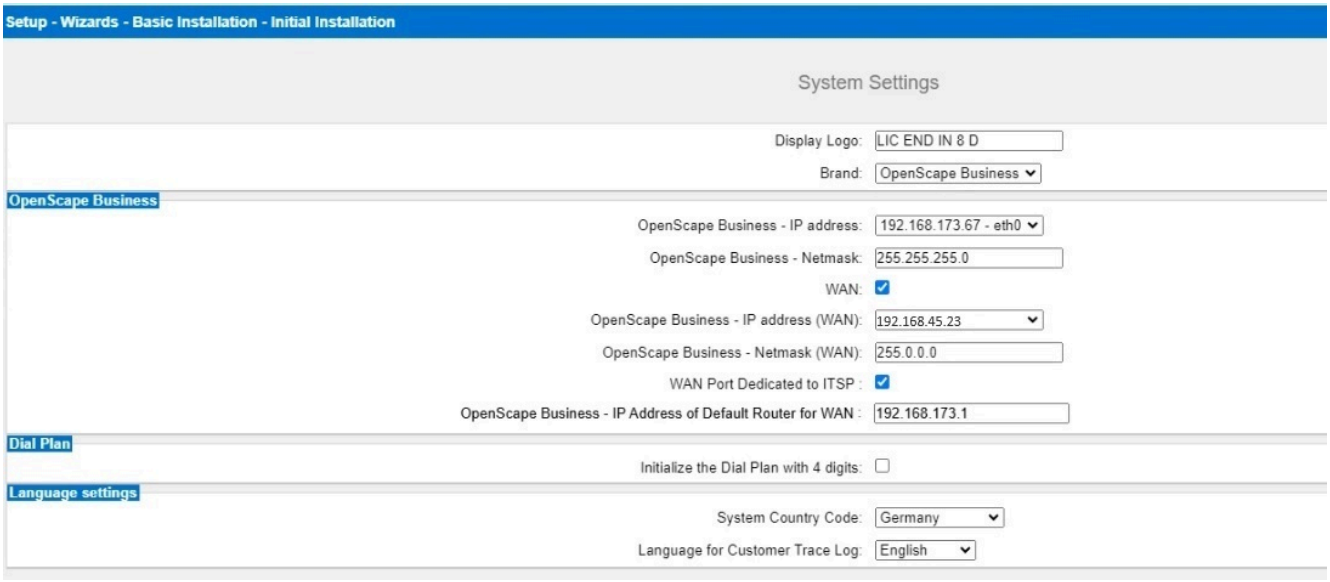
You are in the **System Settings** window of the **Initial Installation** wizard.

Please note that this feature is only applicable for ITSPs that do not require the use of STUN in the provider settings.

Step by Step

1) Enable the **WAN** check box and select the appropriate network interface. The option **WAN Interface Dedicated to ITSP** becomes available.

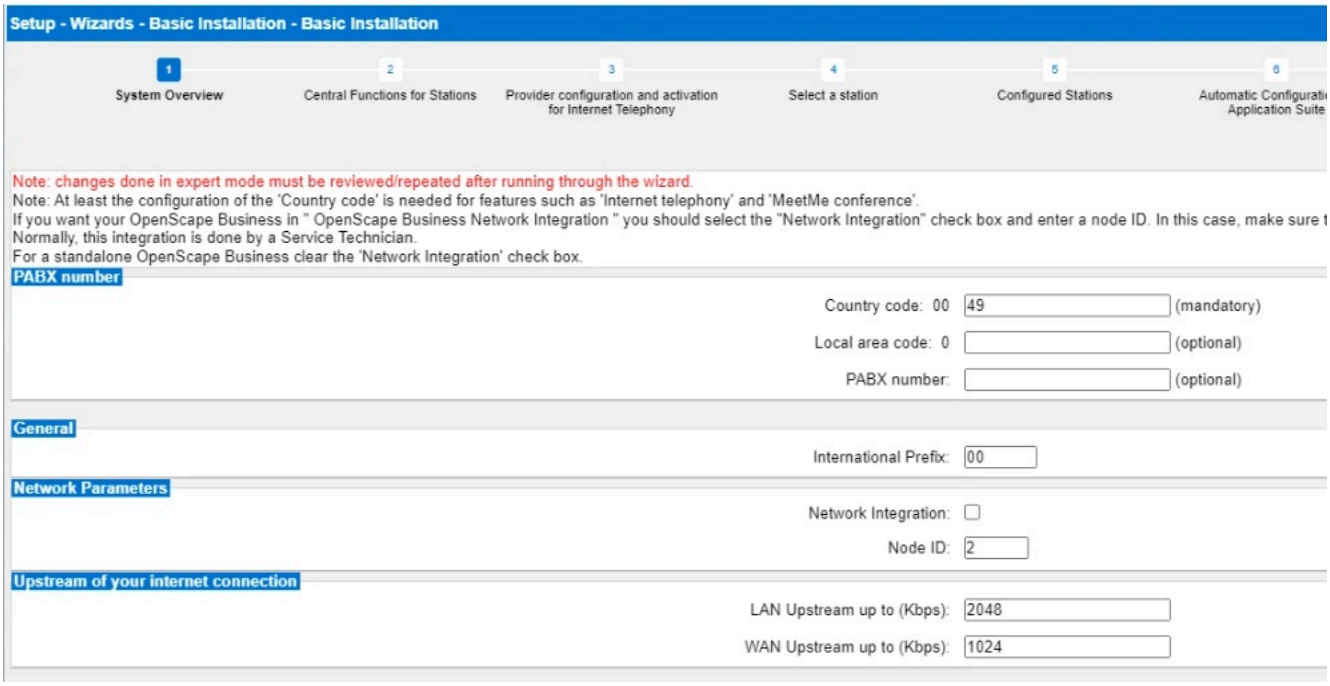
2) Click to enable the **WAN Interface Dedicated to ITSP** check box.



3) Click on **OK & Next**.

4) Navigate to **Setup > Basic Installation** and run the **Basic Installation** wizard.

5) Configure the maximum upstream values in the corresponding **LAN Upstream up to (Kbps)** and **WAN Upstream up to (Kbps)** fields.



6) Click on **OK & Next**.

7) After applying the configuration, a system restart is required.

NOTICE: STUN is not supported on the WAN interface when using the LAN/WAN feature. It is supported only on the LAN interface. If the ITSP requires STUN, SIP traffic must be routed through the LAN interface.

6.7.5 Internet Telephony

The **Provider configuration and activation for Internet telephony** window is used to configure Internet telephony. You can configure predefined or new Internet Telephony Service Providers (ITSPs). You can configure one or several accounts for each ITSP. Up to 8 ITSPs may be active simultaneously.

You have the following options:

- **Configure a predefined ITSP**

  You can use predefined ITSP templates. To do this, the own access data and phone numbers are entered in the template, and this is then activated.
- **Configure a new ITSP**

  You can also add and activate a new ITSP.

  Configuring a new ITSP is seldom required and can be very time-consuming. This option is therefore not described in the initial installation. Detailed information can be found in the chapter Configuring an ITSP .
- **Disable Internet telephony**

  You can disable Internet telephony.

NOTICE: Configuration examples can be found on the Internet at the **Unify Experts Wiki** under *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Assigning the ITSP Phone Numbers

- In the case of an **Internet Telephony Station Connection**, the ITSP provides individual numbers such as 70005555, 70005556, etc. These individual call numbers are then assigned manually as the internal call numbers of the subscribers.
- In the case of an **Internet telephony point-to-point connection**, the ITSP provides a call number range, e.g., (+49) 89 7007-100 to (+49) 89 7007-147. The call numbers from the range are then assigned manually as the internal call numbers of the subscribers.

These two connection types can be combined as appropriate.

Alternatively, the ITSP phone numbers can be entered as the DID call numbers of the subscriber for both connection types during the station configuration.

Internal call number	Name	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

The ITSP call numbers thus result from the configured PABX number (e.g., country code 49) and the entered DID numbers in long format. This has advantages for the digit analysis and call management, even in an internetwork. The ITSP connection is thus DID-enabled for another node, for example.

A further CO trunk connection via ISDN is only possible to a limited extent in this case (useful for emergency calls, for example).

6.7.5.1 How to Configure a Predefined ITSP

Prerequisites

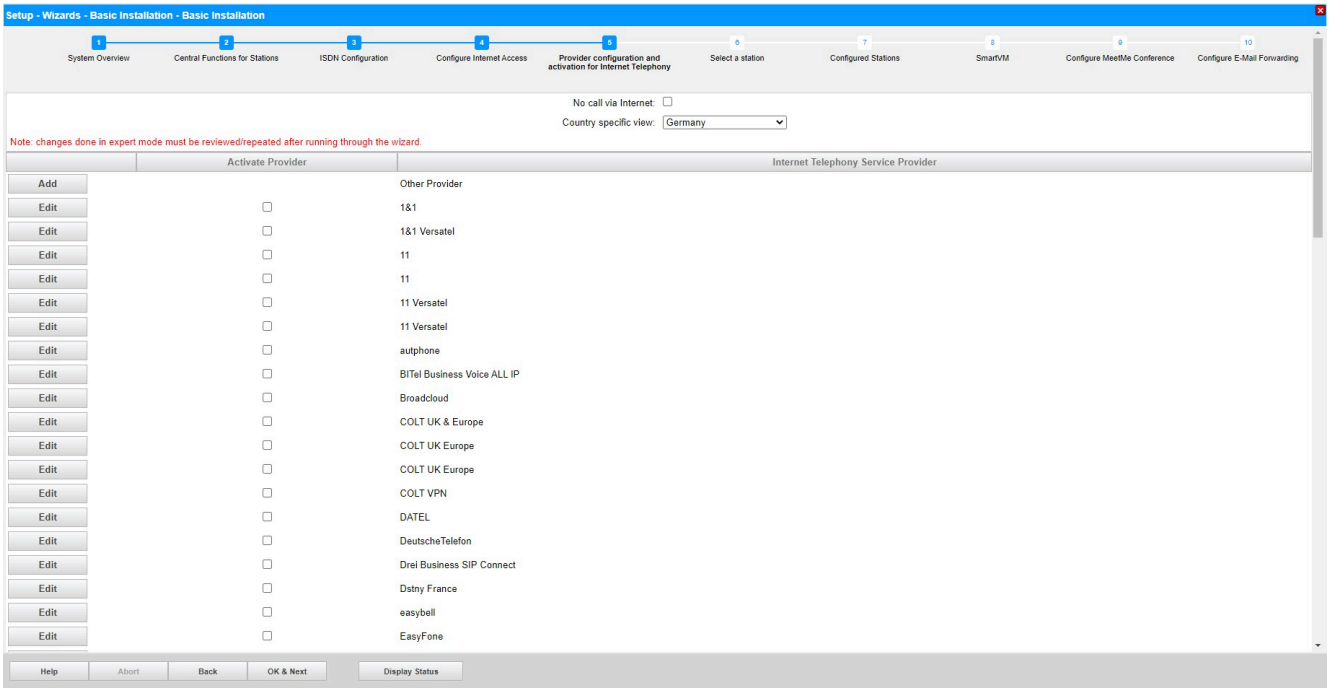
You are in the **Provider configuration and activation for Internet Telephony** window of the **Basic Installation** wizard.

The Internet connection is operational.

Your ITSP's Internet telephony access data is available (for example, user account, password and Internet telephony numbers).

Step by Step

1) Clear the **No call via Internet** check box. A country-specific list of the possible ITSPs is displayed. The list contains the predefined ITSPs for the selected country and any already created ITSPs.



2) If you want to change the preset country, select the desired country from the **Country specific view** drop-down list to display the ITSPs that are available for this country.

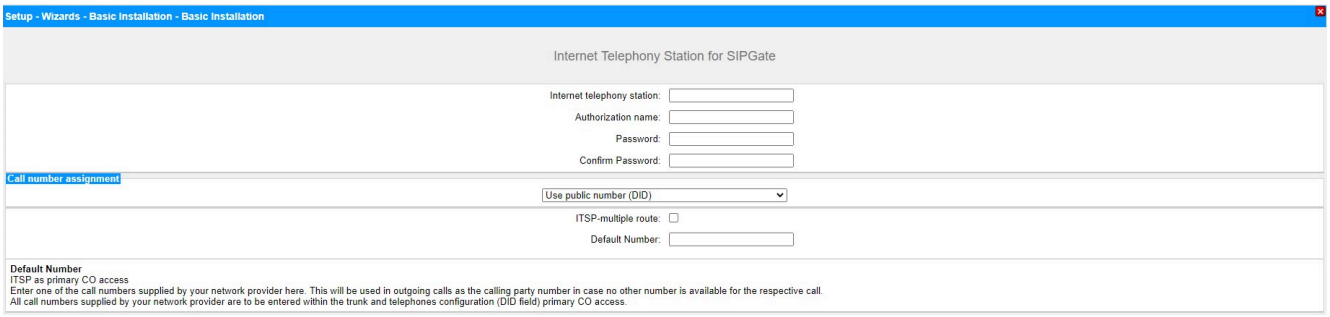
3) If required, click **Display Status** to check which ITSPs have already been activated and which Internet telephony subscribers have already been configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.

4) To configure Internet telephony stations, click **Edit** in the line associated with the relevant ITSP.

5) Activate the check box **Enable Provider**.

6) Click **OK & Next**.

7) Click **Add** to configure your ITSP accounts with the corresponding Internet telephony numbers. The fields that will then be displayed are provider-specific.



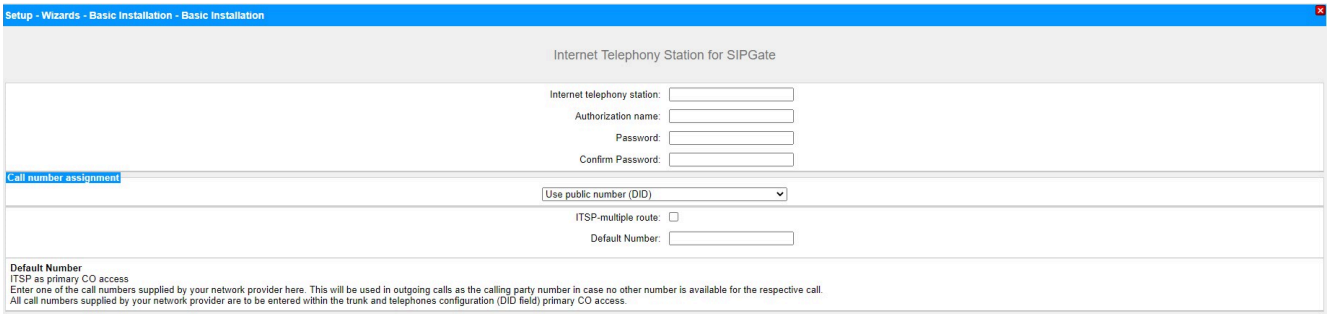
8) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

9) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

10) Enter the password you received from the ITSP in the **New Password** and **Confirm Password** fields. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

11) Assignment of Internet telephony phone numbers - Option 1:

Use public number (DID): the Internet telephony phone numbers of your Internet telephony station connection or Internet telephony point-to-point connection are not entered here during the ITSP configuration, but when the configuring the stations, i.e. the telephones and subscribers (in the **DID** fields).



a) Select the option field **Use public number (DID)** in the **Call number assignment** area.

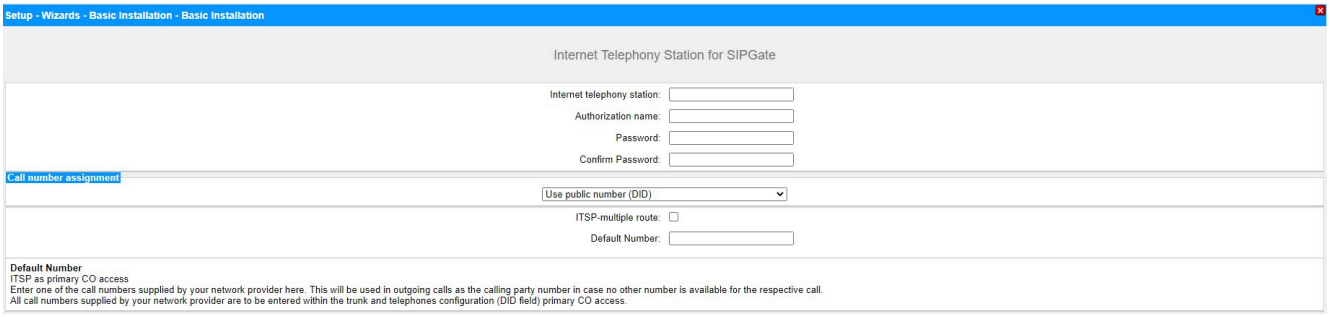
b) Under **Default Number**, enter the phone number to be used for outgoing calls when no caller DID number is available.

c) If your ITSP supports the "Mobile Extension (MEX)" feature, enter the MEX number provided by the ITSP (8 positions, digits only) under **MEX Number**.

12) Assignment of Internet telephony phone numbers - Option 2:

Use internal number (CalIno) / Single entries: You have an Internet telephony station connection and have received individual call numbers as Internet telephony phone numbers (e.g. 70005555, 70005556,...).

Then assign these single numbers to the internal call numbers of the subscribers.



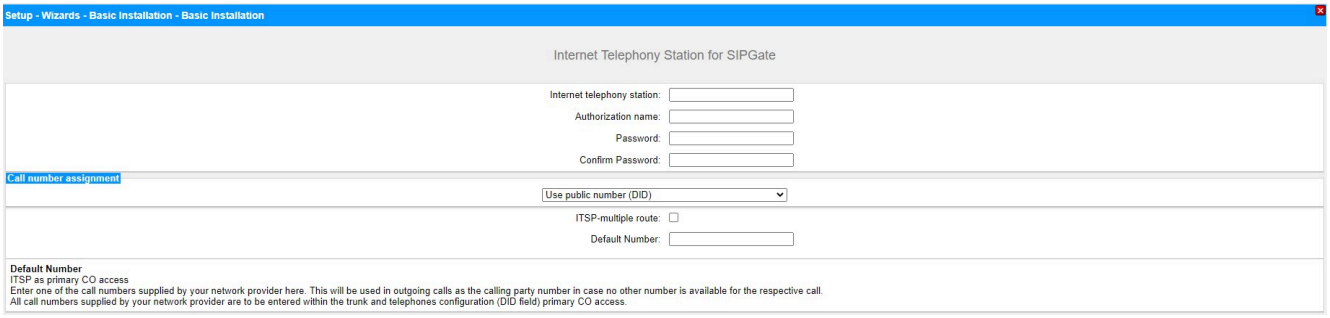
a) Select the option field **Use internal number (CalIno) / Single entries** in the **Call number assignment** area.

b) In the **Internet Telephony Phone Numbers** area, enter one of the Internet telephony phone numbers provided by the ITSP in the field next to the **Add** button and then click **Add**.

c) To assign further Internet telephony numbers to the account, repeat step b).

13) Assignment of Internet telephony phone numbers - Option 3:

Use internal number (CalIno) / Range entry: You have an Internet telephony point-to-point connection and have received a call number range as Internet telephony phone numbers (e.g., +49) 89 7007-100 to (+49) 89 7007-147. You then assign the call numbers from the call number range as the internal call numbers of the subscribers.



a) Select the option field **Use internal number (CalIno) / Range entry** in the **Call number assignment** area.

b) Enter the system phone number under **System phone number (prefix)**.

c) Enter the desired DID number range for the Internet telephony station in the 'from' **and** 'to **' fields after** Direct inward dialing band. The range entered by default is 100 - 147.

14) Click on **OK & Next**.

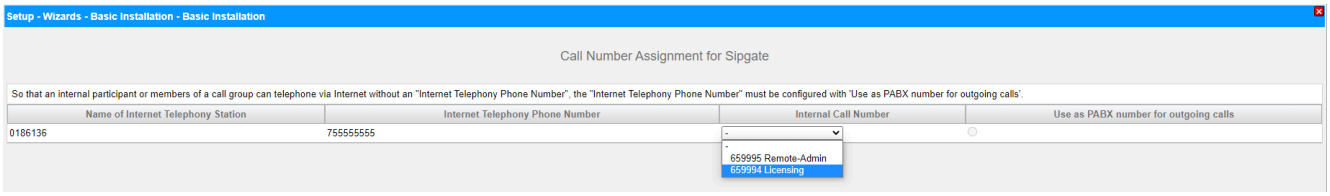
15) If you want to configure additional accounts and their associated Internet telephony numbers, repeat steps 7 through 14.

16) Click **OK & Next**. You will see an overview of which Internet telephony phone numbers are assigned to accounts.

17) Assign one internal station number each to every Internet telephony phone number.

This step is not required if you have selected option 1 for the assignment of the Internet telephony phone numbers. In this case, the assignment

is made when the configuring the stations (i.e., the telephones and subscribers) in the **DID** field.



a) To do this, select an internal call number in the appropriate line from the **Internal Call Number** drop-down list.

b) If subscribers without Internet telephony phone numbers or members of a call group are to be allowed to make external calls via the Internet, the radio button **Use as PABX number for outgoing calls** must be activated. The radio button can be activated for only one single Internet telephony phone number.

18) Click **OK & Next**. Here you see again the list of predefined and newly added ITSPs. The enabled ITSPs are identified with a check mark in the **Enable Provider** column. If you are having connection problems with already activated ITSP, you can register it again with **Restart ITSP**.

19) Click **OK & Next**.

20) Enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field. Please do not confuse this with the download speed!

NOTICE: The number of simultaneous Internet calls permitted is displayed in the **Number of Simultaneous Internet calls** field. If the voice quality deteriorates due to the network load, you will need to reduce the number.

For more information about the number of simultaneous Internet calls, please refer to Limiting the Number of Simultaneous Calls via an ITSP on page 781.

---

21) Click **OK & Next**.

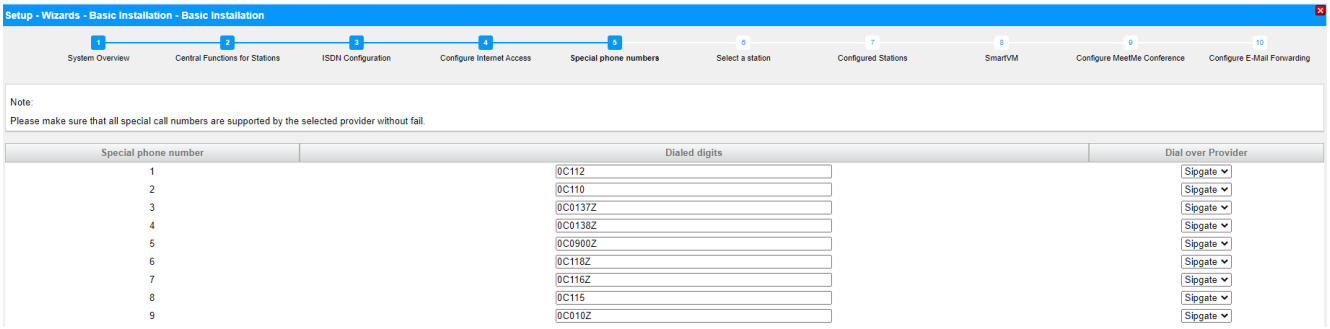
22) If you did not activate the full-time circuit when setting up your Internet access, you can now do this here. Without a permanent connection (full-time circuit), you cannot receive calls over the Internet. If the full-time circuit has already been set up, the fields described under a) to c) will not appear.

a) Enable the radio button **On** under **Full-Time Circuit**.

b) In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be deactivated (e.g., 04:59).

c) Click **OK & Next**.

23) Enter the special numbers you want in the **Dialed digits** column.



The following station number entries are valid:

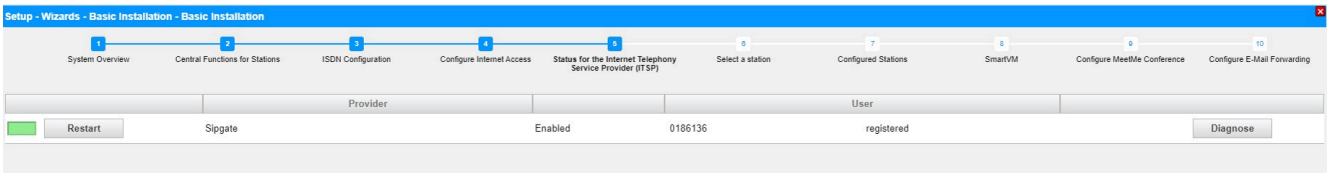
- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

24) Use the **Dial over Provider** column to specify whether the special number should be dialed via ISDN or an ITSP. Only the active ITSP is displayed.

NOTICE: Ensure that emergency numbers can always be dialed. If you want to dial emergency numbers via an Internet Telephony Service Provider, you must make sure that the ITSP supports this feature.

---

25) Click **OK & Next**. The status of your ITSP will be displayed.



The configured ITSPs at which you are already registered are marked in green.

The configured ITSPs at which you are not yet registered are marked in orange.

26) Click **Next** followed by **Finish**.

6.7.5.2 How to Deactivate Internet Telephony

Prerequisites

You are in the **Provider configuration and activation for Internet Telephony** window of the **Basic Installation** wizard.

Step by Step

1) Leave the **No call via Internet** check box selected.
2) Click **OK & Next** twice.

6.7.6 Stations

In the **Select a station - ...** window, you can configure the stations connected to the communication system.

Proceed as follows:

1) Configure the IP and SIP stations

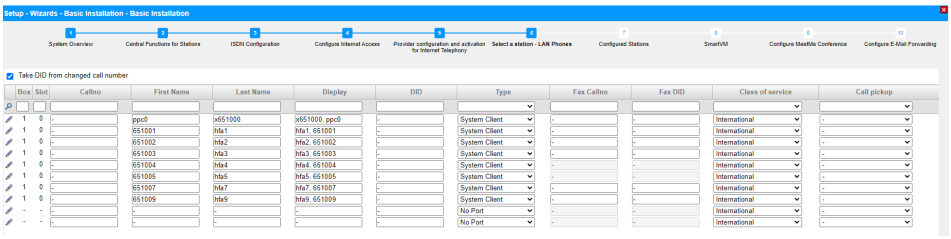
IP and SIP stations include LAN phones or WLAN phones, for example.

6.7.6.1 How to Configure IP and SIP Stations

Prerequisites

You are in the **Select a station - LAN Phones** window of the **Basic Installation** wizard.

A functional wireless LAN network is needed to operate WLAN phones.



Step by Step

1) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

2) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

3) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name`.

NOTICE: The name can consist of up to 16 characters, but should not include any diacritical characters such as

umlauts or special characters. The name specified here will be entered as the Last Name at the UC clients, but can be edited there.

4) Select the type of IP station (e.g., "System Client" or "SIP Client") from the **Type** drop-down list in the row of the desired station.

5) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

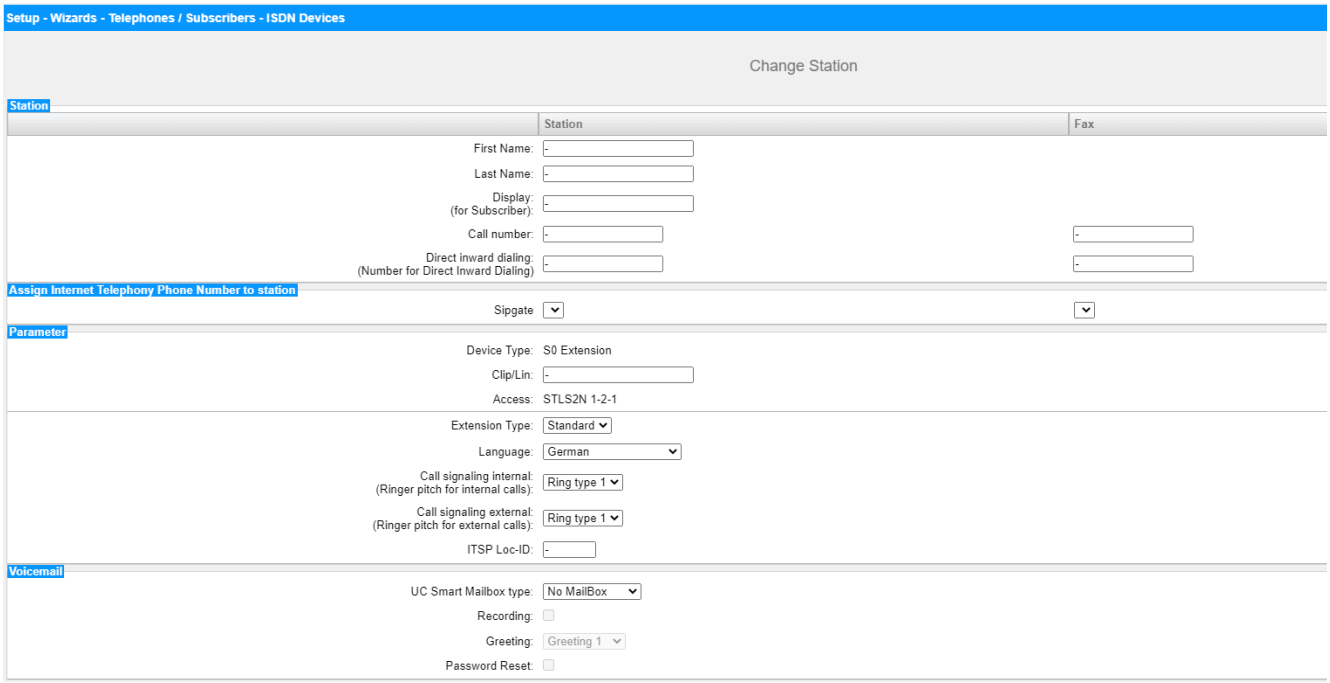
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax Direct Inward Dialing** field in the row of the desired subscriber.

6) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

7) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

8) Make the settings described under this step only if needed or for a SIP phone:

   a) Click in the row of the desired station on the pencil icon **Edit**.



   b) For SIP phones: If the SIP phone is to be operated in conjunction with a dual-mode mobile phone, enter the dialout prefix followed by the telephone number of the mobile phone (e.g., **0016012345678**) in the **Mobility** area under `Mobile phone number`. In addition, select this SIP client from the **Web Feature ID** drop-down list. (see Dual-Mode Telephony).

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

d) Select the language for the menu controls on the phone from the **Language** drop-down list.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Only for SIP phones: Enter the authentication password in the **Password** and **Confirm password** fields.

h) Only for SIP phones: Enter the user ID for the authentication in the **SIP User ID / Username** field.

i) Only for SIP phones: Enter the associated zone for the authentication in the **Realm** field.

j) Click on **OK & Next**.

k) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

l) Click on **OK & Next**.

9) If you want to configure another IP station, click on **Store data** and repeat steps 1 through 8.

10) Click on **OK & Next**. A list of all configured stations appears. This list is effectively a dial plan.

11) If required, click **Print** to print out the data of the configured stations.

12) Then click **OK & Next**.

Related concepts

Multilingual Text Output on page 1172

6.7.7 Configuring UC Suite

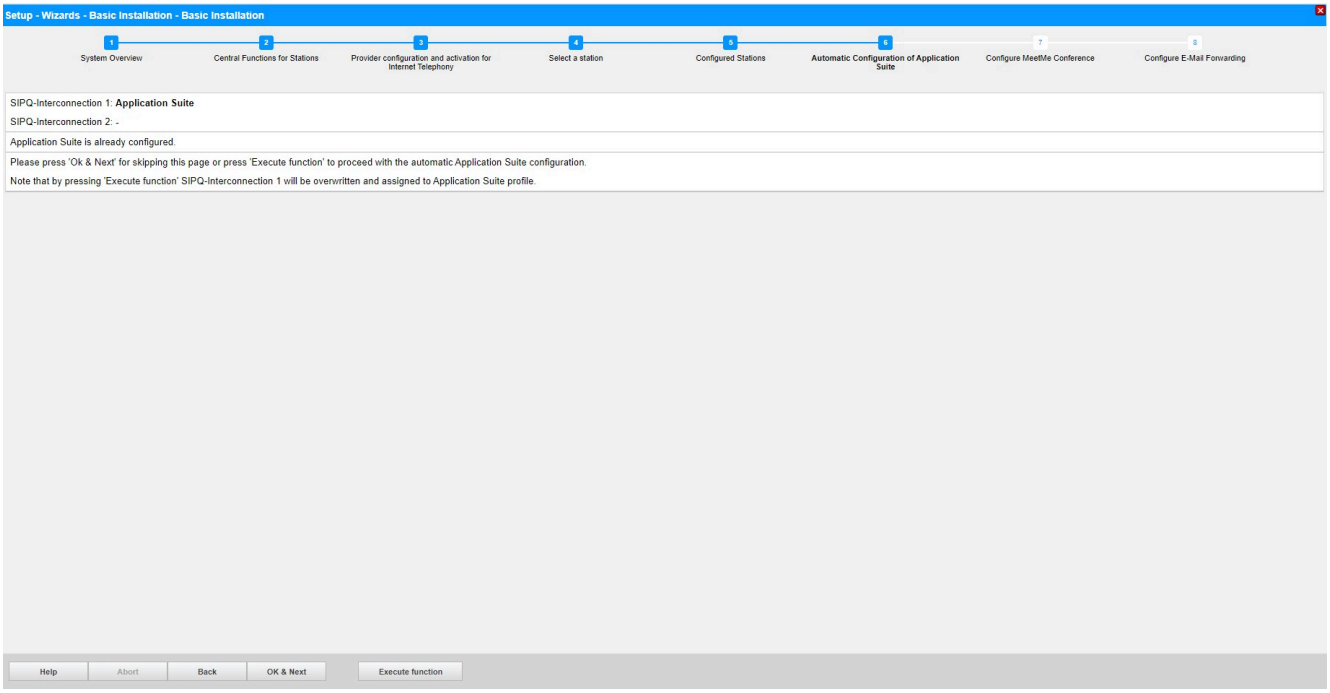
You can perform the automatic configuration of the UC solution UC Suite in the **Automatic Configuration of the Application Suite** window.

NOTICE: This window appears only if **Package with UC Suite** was selected during the application selection in the **Initial Installation** wizard.

6.7.7.1 How to Configure the UC Suite

Prerequisites

You are in the **Automatic Configuration of Application Suite** window.



Step by Step

Click on **Execute function**. The UC Suite is configured automatically. Once the progress bar shows 100%, click on **OK & Next**.

NOTICE:

For OpenScape Business S the wizard automatically generates 60 media channels in UC Suite. In parallel 16 channels for announcement can be used without configuration of additional media channels.

6.7.8 Configuring UC Smart Mailboxes

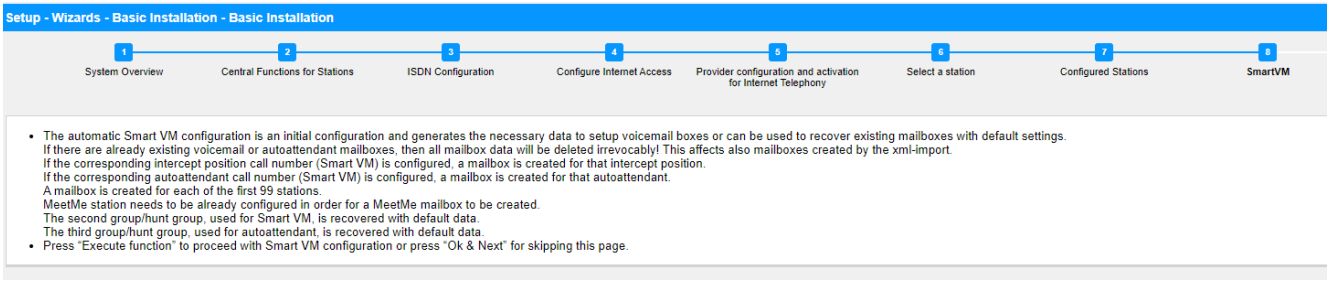
If you are using the UC solution UC Smart, you can perform the automatic configuration of the UC Smart voicemail boxes (Smart VM, Smart VoiceMail) in the **Automatic Configuration of Smart VM** window.

NOTICE: This window appears only if **Package with UC Smart** was selected during the application selection in the **Initial Installation** wizard.

6.7.8.1 How to Configure UC Smart Voicemail Boxes

Prerequisites

You are in the **Automatic Configuration of Smart VM** window.



Step by Step

1) If the UC Smart voicemail boxes are not to be used, click on **OK & Next**. The configuration of the voicemail boxes will be skipped.
2) If the UC Smart voicemail boxes are to be used, click on **Execute function**. Voicemail boxes are then automatically configured for the first 100 subscribers. Once the progress bar shows 100%, click on **OK & Next**.

NOTICE: Existing UC Smart or UC Smart AutoAttendant voicemail boxes are irrevocably deleted in the process.

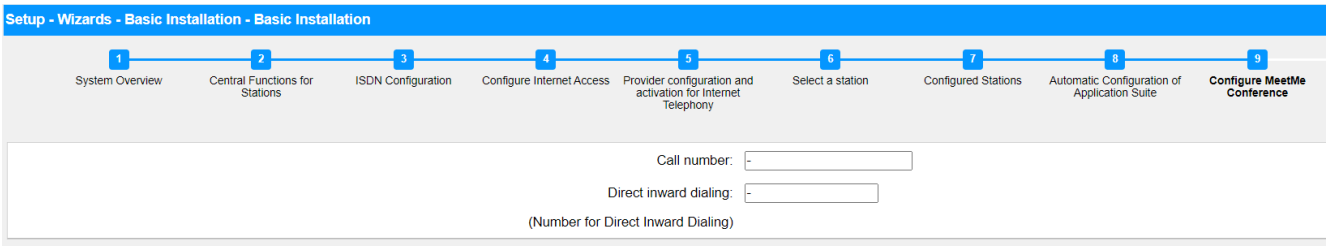
6.7.9 Conference Server Settings

The **MeetMe Conference** settings window can be used to define the call numbers and the dial-in numbers for conferences.

6.7.9.1 How to Edit the Conference Server Settings

Prerequisites

You are in the **Configure MeetMe Conference** window of the **Basic Installation** wizard.



Step by Step

1) Enter a phone number for the conference in the **Phone Number** field.
2) Enter the dial-in number for the conference (conference DID) with which subscribers can dial into an existing conference in the **Direct inward dialing** field.
3) Click on **OK & Next**.

6.7.10 E-mail Delivery (Optional)

You can configure the delivery of e-mails in the **Configure E-Mail Forwarding** window. These e-mails notify users of voicemail and fax messages and administrators of system messages.

You have the following options:

- Configuring the Sending of E-mails

  You can specify an external E-mail server via which the e-mails are to be sent by OpenScape Business. Voicemails, fax messages and internal system messages can then be sent via this E-mail server to one or several different configurable e-mail addresses.

  NOTICE: Entering the e-mail server is important if an e-mail with a link to the installation file(s) is to be automatically sent to the users of the UC Suite.

6.7.10.1 How to Configure the Sending of E-mails

Prerequisites

If the external E-mail server has been configured to use basic authentication, make sure an e-mail account with a password exists with an e-mail provider, and you know the access data for this account.

If the external E-mail server has been configured to use modern authentication (Microsoft OAuth 2.0 token-based authorization), as in the case of Exchange Online, make sure that:

- The sender's email account must be allowed to use Authenticated SMTP (by default this option is inactive in Microsoft 365 tenant). Once Authenticated SMTP is activated, the OAUTH 2.0 email forwarding works normally with all OpenScape Business mainboards.

- An application with the required permissions has been registered in Microsoft Azure Active Directory (Azure AD) for your OpenScape Business system to send emails.
- You know the Application (client) ID and the Directory (tenant) ID of the registered application.

  Ask your Azure AD administrator to provide these values, if required.
- The email address that will appear as the sender of the emails belongs to the same Azure AD or tenant as the registered application.

You are in the **Configure E-Mail Forwarding** window of the **Basic Installation** wizard.

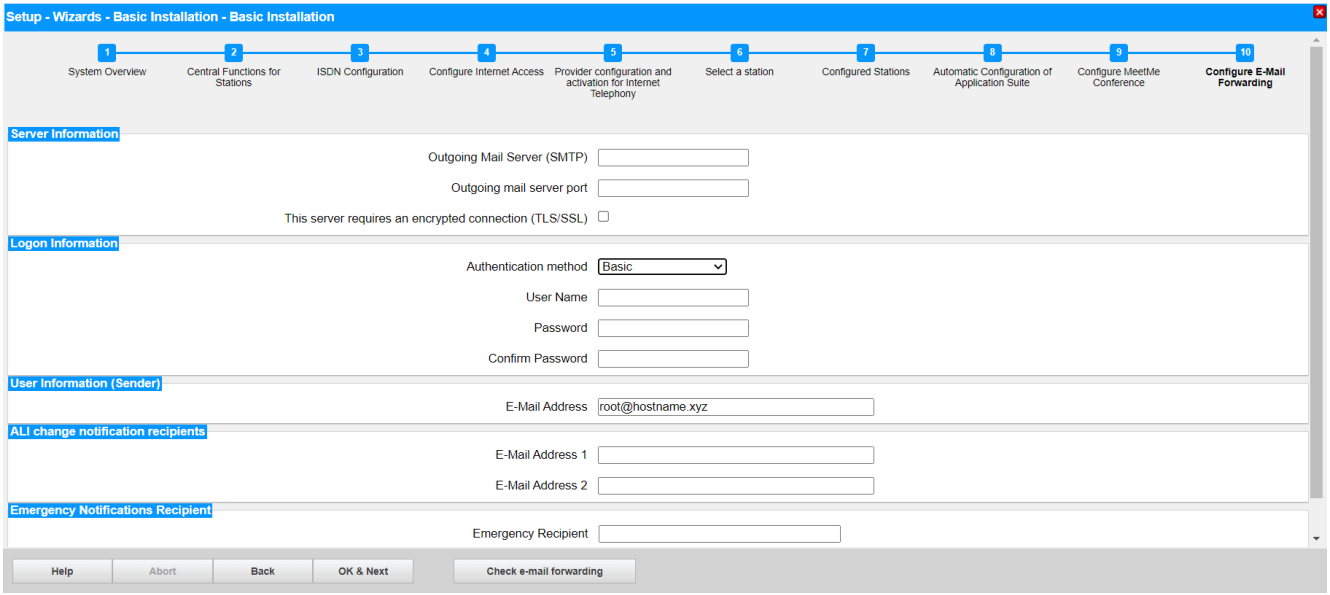


Figure 7: E-mail forwarding options when basic authentication method is selected

Step by Step

1) Enter the **Outgoing mail server (SMTP)** for the e-mail server to be used for sending e-mails, e.g., `smtp.web.de`. Ask your e-mail provider for the outgoing mail server if required.

   NOTICE: Make sure that the name of the outgoing mail server can be resolved. If not, you must start the e-mail sending function via **Service Center** > **E-mail Forwarding** and then enter the IP address of the outgoing mail server instead of its name.

2) Enter the **Outgoing mail server port** for the server port to be used for sending e-mails. Ask your e-mail provider for the outgoing mail server if required.
3) If a secure connection is required, enable the **This server requires an encrypted connection (TLS/SSL)** check box. If required, check with your e-mail provider whether this option needs to be enabled.

4) If the external E-mail server has been configured to use basic authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Basic**.
   b) Enter the **User Name** of the e-mail account, e.g.,: `john.doe`.
   c) Enter the **Password** for the e-mail account and repeat it in the **Confirm Password** field.
5) If the external E-mail server has been configured to use modern authentication, proceed as follows:
   a) From the **Authentication method** drop-down list, select **Microsoft OAuth 2.0**.
   b) Enter the Application (client) ID obtained from the Microsoft Azure portal in the **Application ID** field.
   c) Enter the Directory (tenant) ID obtained from the Microsoft Azure portal in the **Tenant** field.
6) Enter the **E-mail Address** that will appear as the sender of the emails, for example: `john.doe@web.de`.
7) Enter the **E-mail Address 1** to get a notification email when ALI tolerance has been used. You may also enter a second email address in the **E-mail Address 2** field.
8) In the **Emergency Recipient** field, enter the e-mail address of an on-site security officer to which an e-mail is sent when an emergency number is dialed.

   The subject of the e-mail will be "New emergency call". The call number and the name of the caller, if configured, are included in the e-mail which are retrieved from the database of the system.
9) If you have selected **Microsoft OAuth 2.0** as authentication method, proceed as follows:
   a) Click on **OK & Next**.
   b) Wait for an authorization link and user code to appear.

      The authorization code expires after some minutes.
   c) Open the authorization link and enter the user code on the pop-up.
   d) Sign in with the email address you have entered in step 6 on page 247 (**E-mail Address**).

      The email address must be in the same Azure AD or tenant as the registered application.
   e) After successful authentication, the pop-up displays a message as below:

      `You have signed in to the <application-name> on your device. You may now close this window..`
   f) Close the pop-up and return to WBM. If the authentication was successful, you will see the message `The authentication was successful!.`

10) If you want to check the entered e-mail settings, proceed as follows:
    a) Click on **Check e-mail forwarding**.
    b) Under **Send to e-mail address**, enter the e-mail address of any e-mail box that you can access. The test e-mail will be sent to that e-mail address.
    c) Under **Subject in the e-mail**, enter a descriptive text so that you can identify the e-mail in your e-mail inbox.
    d) Click on **Send Test E-mail**. The e-mail settings are verified, and the e-mail is sent to the specified e-mail address.
    e) Check whether the e-mail has arrived in your e-mail inbox.
    f) If the e-mail was sent correctly, click **Back** and proceed to the next step.
    g) If the e-mail delivery failed, click **Back** and correct your e-mail settings.
11) Click on **OK & Next** followed by **Finish**. The basic installation is finished. Before you perform the backup mentioned in the wizard, you should activate the licenses.

6.8 Closing Activities

After the initial installation and the basic installation with the WBM have been completed, some important settings must still be made for the operation of OpenScape Business.

Proceed as follows:

1) Activate and assign licenses

   The licenses procured with OpenScape Business must be activated within a period of 30 days. The time period begins the next time you log on to the WBM. After this time period expires, the communication system will only operate in restricted mode. Once the licenses have been activated successfully, they must be assigned to the stations and lines. System-wide features are enabled automatically upon activation.
2) Provision the UC Smart client for installation (only for UC Smart)
3) Provision the UC Clients for installation

   The UC clients are part of the UC Suite. The installation files for the UC Client are accessible via the WBM and can be made available to the IP stations automatically or manually.

   In addition, the administrator has the option of performing a silent installation. The silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC Suite PC clients on a PC without requiring any further user inputs. For more information, see Silent Installation/Uninstallation for UC Suite PC Clients.
4) Perform a data backup

   All previous changes to OpenScape Business must be backed up. The backup can be stored as a backup set in the internal network, for example.

6.8.1 How to Activate and Assign the Licenses

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

You know the LAC (License Authorization Code) for releasing the license and have a user ID and password for accessing the license server.

You need Internet access to connect to the license server.

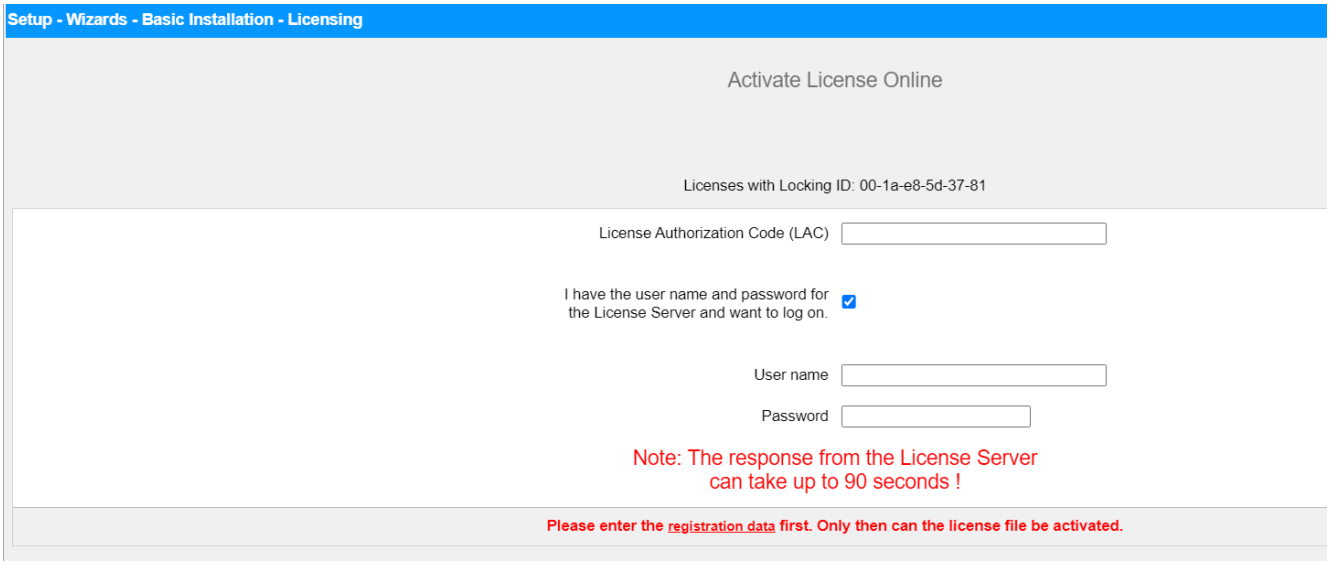
Step by Step

1) Activate license online:

a) In the navigation bar, click on **Setup**.

b) In the navigation tree, click **Wizards** > **Basic Installation**.

c) Click on **Edit** to start the **Licensing** wizard.



d) Enter the appropriate LAC in the **License Authorization Code (LAC)** field.

e) Select the check box **I have the user name and password for the License Server and want to log on**.

f) Enter the **User Name** and **Password** for logging into the License Server.

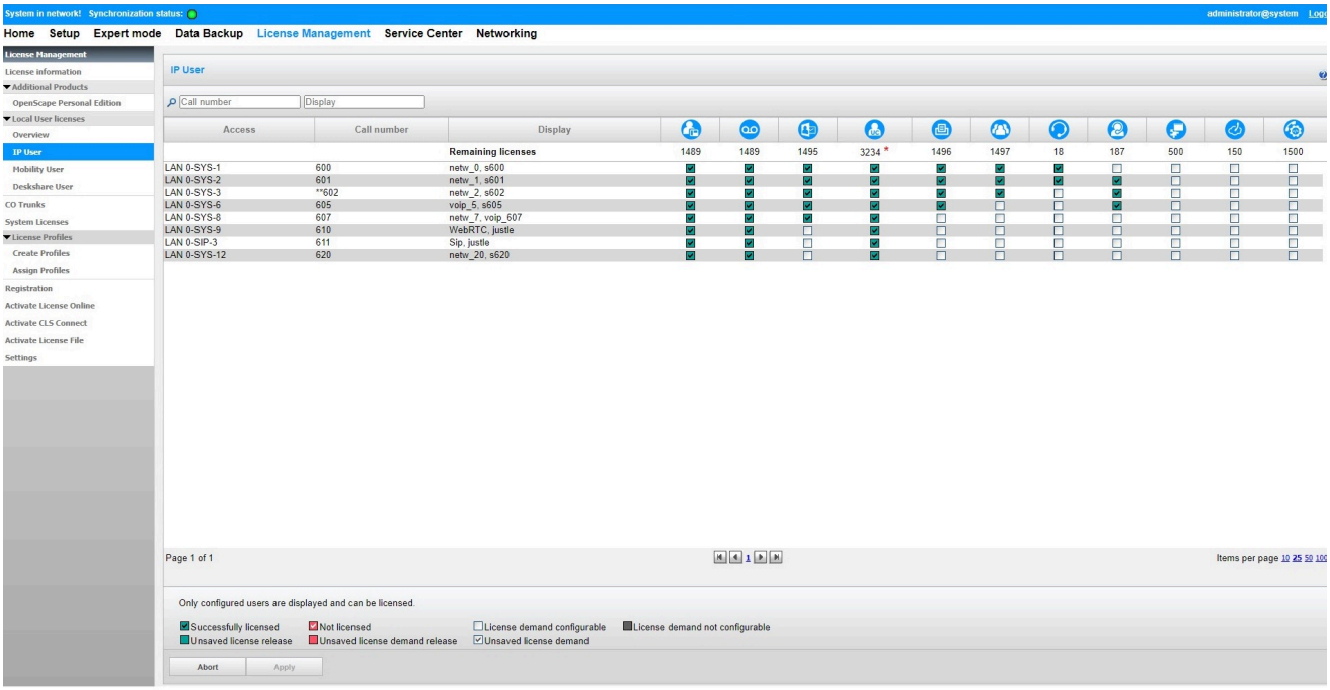
g) Click on **OK & Next**. The connection to the license server is established, and the licenses are released.

2) Assign licenses to stations:

a) Click on **License Management** in the navigation bar.

b) In the navigation tree, navigate to the desired type of subscriber under **Local User Licenses** > **...**. You will be shown a list of all subscribers of the selected subscriber type.

c) In the row of the desired subscriber, select the check box in the **User license** column (first column with check boxes).



d) Activate the user-oriented licenses in the row of the desired subscriber by selecting the appropriate check boxes.

NOTICE: User-oriented licenses can be assigned to a subscriber only if a station license (user license) was assigned to the subscriber earlier (step c).

---

e) Click on **OK & Next**. A check is performed to determine whether there are enough licenses for your assignment.

If sufficient licenses are available, the licensing of the subscriber is completed.

f) If licenses are missing, the errors are indicated by displaying a check box shaded in red. Correct these errors and repeat step e.

3) Assign licenses to trunks:

a) In the navigation tree, click **CO trunks**. The number of trunk licenses purchased will be displayed in the **CO trunks** area.

b) For SIP trunks: In the **License demand for number of simultaneous Internet calls in this node** area, enter the number of Internet calls that can be conducted simultaneously via an ITSP.

c) Click on **OK & Next**.

6.8.2 How to Provision the UC Smart Client for Installation

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The hardware and software for using UC @work are available.

NOTICE: Licenses are required to use the UC Smart client myPortal @work.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Software** in the navigation tree.
3) Click on the Download icon of **myPortal @work** and save the installation file on a shared network drive.
4) Send the two installation files to the users of myPortal @work.
5) Alternatively, you can also send the users of myPortal @work the link with which they can access the installation file:

```
https://<IP address of the communication system>/
management/downloads/myPortalAtWorkSetup.exe
```

6.8.3 How to Provision the UC Suite Clients for Installation

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The hardware and software for using the UC Suite are available.

NOTICE: Licenses are required to use the UC Suite clients.

Step by Step

1) To enable the installation files to be provided automatically to a station, make sure that the following steps have been performed:
   a) The e-mail addresses of the stations and the associated subscriber data must have either been already imported via an XML file or entered later under **Setup** > **UC Suite** > **User Directory**.
   b) An e-mail server must have been specified.

   NOTICE: You can also enter an E-mail server later under **Service Center** > **E-mail Forwarding**.

   All subscribers whose e-mail addresses are known receive an e-mail with a link to the installation directory of the UC clients and Getting Started Instructions. The installation folder also includes a Readme file with information on installing the software on client PCs.

2) If the required steps for automatic notification are not fulfilled, you can also make the installation files available manually. To do this, proceed as follows:
   a) Click on **Service Center** in the navigation bar.
   b) Click on **Software** in the navigation tree.
   c) Click on the desired UC client and save the zipped installation file on a shared network drive.
   d) Click in the navigation tree on **Documents** and select **User Documentation** from the drop-down list.
   e) Click on the documentation of the desired UC client and save the documentation file on a shared network drive.
   f) Send the zipped installation file and the documentation file to the users of the UC clients by e-mail or inform the users about the storage location of these files.
   g) The zip file with the installation files also includes a Readme file. Notify the users that the installation of the UC clients must be performed in accordance with the installation notes in the Readme file.
3) Alternatively, you can also send the UC users links through which they can directly access the installation files of the UC clients.
   a) Click on **Service Center** in the navigation bar.
   b) Click on **Software** in the navigation tree.
   c) Click on the **Show Application Links** button. You will be presented with multiple links, depending on the used operating system and the desired UC client. For example:

   ```
   https://<IP address of the communication system>/
   management/downloads/install-common.zip
   ```

6.8.4 How to Perform a Data Backup

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

NOTICE: For more information on backing up data, see Immediate Backup .

Step by Step

1) Click on **Backup and Restore** in the navigation bar.
2) In the navigation tree, click **Backup - Immediate**.
3) Enter a comment for the backup set in the **Comment** field in the **Name** area so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) Activate the target drive on which the backup set is to be saved (e.g., a network drive) in the **Devices** area.
5) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.
6) The backup was successful if the message **Backup completed successfully!** appears. Click on **Finish**.
7) This completes the initial startup with WBM. Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

6.9 Commissioning of IP Phones

The commissioning of IP phones can be facilitated by the existence of a DHCP server that supplies an IP phone with important (network-specific) data that is needed to log into the communication system.

Network-Specific Data

In order to log into the communication system, an IP phone requires some network-specific data. This data can be stored in the DHCP server or be entered directly at the IP phone. The advantage of a DHCP server is that all connected IP phones are automatically supplied with the relevant data.

The following data is required by the IP phone:

- IP address of the communication system
- IP address of DLS server

In addition, the IP phone needs its own call number. This must be entered manually when logging in at the phone.

Registration of SIP Phones

For security reasons, it is recommended that SIP phones register at the communication system. To do this, the registration information on the IP phone and the communication system must match.

The following data is required for the login:

- SIP user ID
- SIP password
- SIP realm (optional)

Use a non-trivial SIP password that complies with the following rules:

- At least 8 characters
- At least one uppercase letter (A - Z)
- At least one lowercase letter (a - z)
- At least one digit (0-9)
- At least one special character

Use a SIP user ID that does not include the phone number.

NOTICE: More information on configuring SIP telephones can be found at `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Using the Internal DHCP Server

If the internal DHCP server of the communication system is used, the network-specific data will already be stored there. In order to enable an IP phone to register at the communication system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server with Network-specific Data

If an external DHCP server is used, the network-specific data must be stored there. In order to enable an IP phone to register at the communication

system, only the specified call number must be entered at the IP phone. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

Using an External DHCP Server without Network-specific Data

If an external DHCP server in which the network-specific data cannot be stored is used, this must be entered at the IP phone. To enable an IP phone to register at the communication system, the defined call number and IP address of the communication system must be entered at the phone, and the settings for the Deployment Service may need to be changed. In the case of SIP phones, the SIP registration data at the SIP phone and at the communication system must match.

6.9.1 How to Configure an IP Phone

Prerequisites

The IP phone is connected to the internal network and operational.

NOTICE: The sample configuration described here uses an OpenStage 40/60/80 IP system telephone. The same settings must also be made for any other IP phone. For more information, refer to the manual supplied with your IP phone.

Step by Step

1) To reach the administration mode of the IP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Admin` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the IP system telephone can be updated automatically. This applies only to IP system telephones. Proceed as follows:

a) Scroll to `Network` and confirm your selection with the OK key.

b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.

c) Scroll to `DLS address` and confirm your selection with the OK key.

d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.

e) Scroll to `Save & Exit` and confirm your selection with the OK key.

f) Scroll to `IPv4 configuration` and confirm your selection with the OK key.

g) Scroll to `Route (default)` and confirm your selection with the OK key.

h) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
i) Scroll to `Save & Exit` and confirm your selection with the OK key.
j) Navigate one menu level back with the Back key.

6) Specify the call number of the phone:
a) Scroll to `System` and confirm your selection with the OK key.
b) Scroll to `Identity` and confirm your selection with the OK key.
c) Scroll to `Terminal number` and confirm your selection with the OK key.
d) Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.
e) Scroll to `Save & Exit` and confirm your selection with the OK key.

7) Navigate one menu level back with the Back key.

8) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

6.9.2 How to Configure a SIP Phone

Prerequisites

The SIP phone is connected to the customer LAN and operational.

NOTICE: The configuration described here uses an OpenStage 40/60/80 SIP system telephone as an example. The same settings must also be made for another SIP phone. For more information, refer to the manual supplied with your SIP phone.

Step by Step

1) To reach the administration mode of the SIP system telephone, press the appropriate key for the Settings/Applications menu on the phone.

2) Scroll through the `Settings` options until `Administrator (Admin)` and confirm this with the OK key.

3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.

4) If you are using the DHCP server of the communication system in the internal network, skip the next step.

5) If you are not using the DHCP server of the communication system in the internal network, you will need to enter the IP addresses of the Deployment Server (DLS) and the communication system so that the software of the SIP system telephone can be updated automatically. This applies only to SIP system telephones. Proceed as follows:
a) Scroll to `Network` and confirm your selection with the OK key.
b) Scroll to `Update service (DLS)` and confirm your selection with the OK key.
c) Scroll to `DLS address` and confirm your selection with the OK key.
d) Specify the IP address of the communication system (`192.168.1.2` by default) as the Deployment Server and confirm your entry with the OK key.

e) Scroll to `Save & Exit` and confirm your selection with the OK key.
f) Scroll to `IPv4 configuration` and confirm your selection with the OK key.
g) Scroll to `Route (default)` and confirm your selection with the OK key.
h) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
i) Scroll to `Save & Exit` and confirm your selection with the OK key.
j) Navigate one menu level back with the Back key.

6) Specify the SNTP time settings:

a) Scroll to `Date and time` and confirm your selection with the OK key.
b) Scroll to `Time source` and confirm your selection with the OK key.
c) Scroll to `SNTP IP address` and confirm your selection with the OK key.
d) Specify the IP address of the communication system (`192.168.1.2` by default) and confirm your entry with the OK key.
e) Scroll to `Timezone offset` and confirm your selection with the OK key.
f) Enter the deviation between the local time and UTC (Universal Time Coordinated) in hours (Germany: `1`) and confirm this with the OK button.
g) Scroll to `Save & Exit` and confirm your selection with the OK key.
h) Navigate one menu level back with the Back key.

7) Specify the call number of the phone:

a) Scroll to `System` and confirm your selection with the OK key.
b) Scroll to `Identity` and confirm your selection with the OK key.
c) Scroll to `Terminal number` and confirm your selection with the OK key.
d) Enter the set phone number (e.g., `120`) and confirm your selection with the OK key.
e) Scroll to `Save & Exit` and confirm your selection with the OK key.

8) Specify the SIP authentication data:

a) Scroll to `Registration` and confirm your selection with the OK key.
b) Scroll to `SIP Session` and confirm your selection with the OK key.
c) Note the `Realm`, or enter a new realm (e.g., `OSBIZ-SIP`), if necessary.
d) Note the `User ID`, or enter a new user ID (e.g., `SIP-120`), if necessary.
e) Specify a `Password` for registering at the SIP server.
f) Scroll to `Save & Exit` and confirm your selection with the OK key.

9) Use the Back key to go back to the `Admin` menu.

10) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

6.10 Uninstalling the Communication Software

The software communication can be uninstalled via a text console.

6.10.1 How to Uninstall the Communication Software

Step by Step

1) Open a terminal (e.g., a GNOME terminal).
2) Enter the command `su` (for superuser = root) in the shell interface and confirm it by pressing the Enter key.
3) Enter the password for the "root" user in the shell interface and confirm it by pressing the Enter key.
4) Enter the command `oso_deinstall.sh` in the shell interface and confirm it by pressing the Enter key. Follow the instructions of the uninstallation program.

6.11 Used Ports

The OpenScape Business system components use different ports, which may need to be opened in the firewall as required. For the ports of the web-based clients (e.g., myPortal to go), port forwarding must be configured in the router.

An actual and complete list of all used ports of OpenScape Business is available in the "Interface Management Database" (IFMD) which can be accessed via the Partner Portal of Unify (https://unify.com/en/partners/partner-portal.

NOTICE: The ports identified with "O" in the list below are optional, i.e., are not permanently open in the firewall.

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
System components							
Admin Portal (https)	X		443	X	X	X	X
CAR Alive checks	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (up to V3R3) 7780, 7791 (V3R3.1 and higher)	O		O	
Communication Client Installer	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

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (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			
LDAP server	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
OpenScape Business status server	X		8808	X		X	X
OpenScape Business user portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (embedded)		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	

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
SNMP (traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Web-based clients							
Web-based clients (http)	X		8801	X	X	X	X
Web-based clients (https)	X		8802	X	X	X	X

NOTICE: For security reasons, we recommend that only https be used for the web-based clients and that port forwarding be set up from external TCP/443 to internal TCP/8802.

CLS certificate

Starting with V3R3.1, a new CLS certificate with an updated Common Name (CN) is provided via a newly introduced port. This offers an improved and stronger digest algorithm as well as updated legal entities. Systems licensed online via CLS Connect mode, require the following two prerequisites:

- The IP address 188.64.16.4 is enabled for outgoing traffic in the firewall.
- Ports 7780 and 7791 are enabled for outgoing traffic in the firewall.

The previously used port 7790 can be removed from the firewall configuration after the upgrade to V3R3.1 to increase security.

6.12 How to collect diagnostic traces for error incident

You can automatically collect the necessary diagnostic traces data for an error incident. 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.

Perform the following steps to collect the diagnostic trace data for the error incident:

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click on **Edit** next to **Error Management**.

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.

   For more information about the traces, see the Troubleshooting guide.
6) Click **OK & Next**.
7) A list with additional information, relevant documentation and hints is displayed. Click **OK & Next**.
8) The scenarios and type of traces that you will collect are displayed. Click **Finish**.
9) Continue by executing the problematic scenario.
10) Once you complete the scenario navigate again to **Setup > Error Management** and click **Edit**.

    You are redirected to the Step 2 of the diagnostic traces collection. If you want to stop the process and initiate it again you can click the **Abort** button.
11) Click **OK & Next**.
12) Enter the required information and click **OK & Next**.
13) A list with necessary information and some further actions is displayed.
14) Click **OK & Next**.
15) Click **Finish** to start downloading the diagnostic trace data.

6.13 Reflashing

Following the steps below you can easily change the software type of a device.

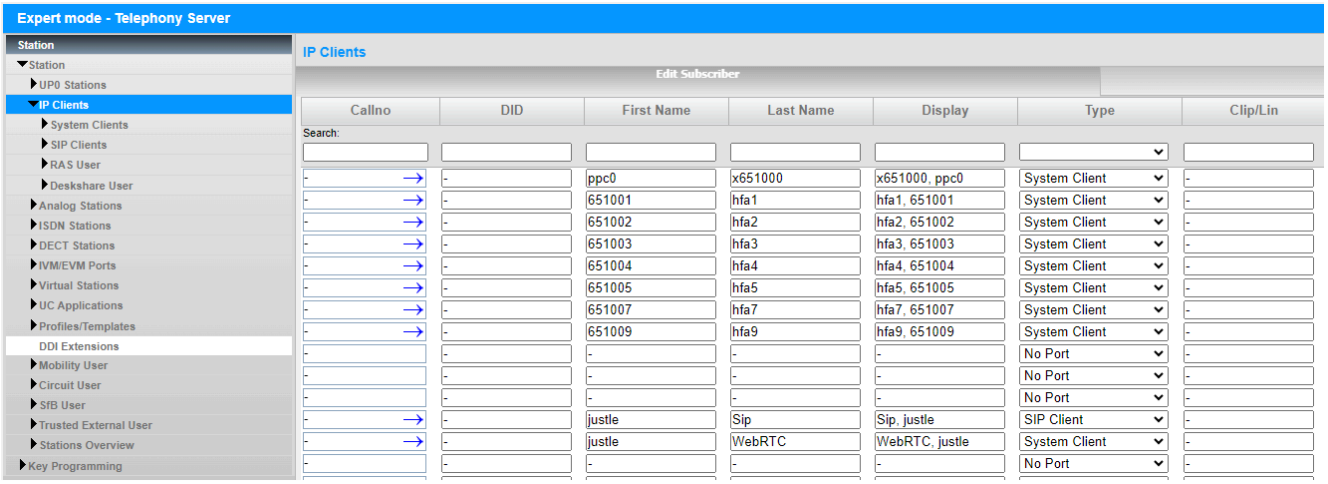
The concept behind this feature is to simplify the way of getting a SIP device (out of the box) and registering it to OSBiz system as an HFA device. The only requirements are:

- the phone must get the DLI address (either from DHCP server or manually)
- the administrator must enter the phone's number (which must be preconfigured as a System Client)

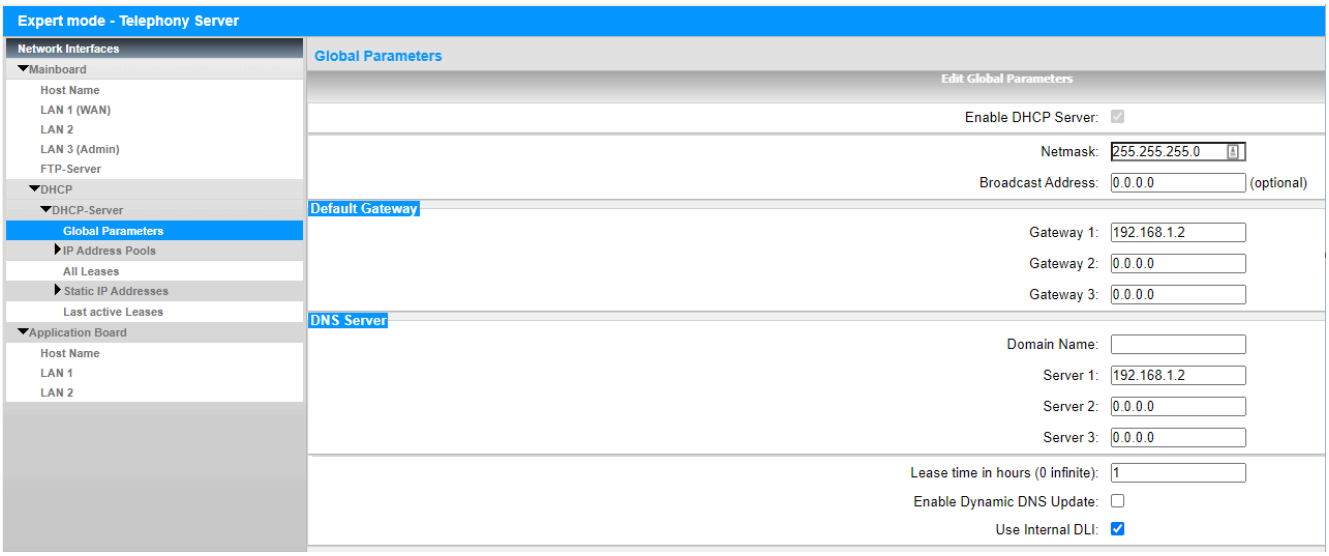
Once the customer gets a new device it will be preconfigured as a SIP device(factory settings). The steps to reflash this device to an HFA device are as follows:

Step by Step

1) Configure in the OSBIZ database the desired phone number as a System Client (HFA).



2) Configure the DHCP server to send the IP address of DLI. This can be done either at the external DHCP Server or the internal DHCP server.



3) If there is no DHCP server used, then you must configure the DLI IP on the phone manually.

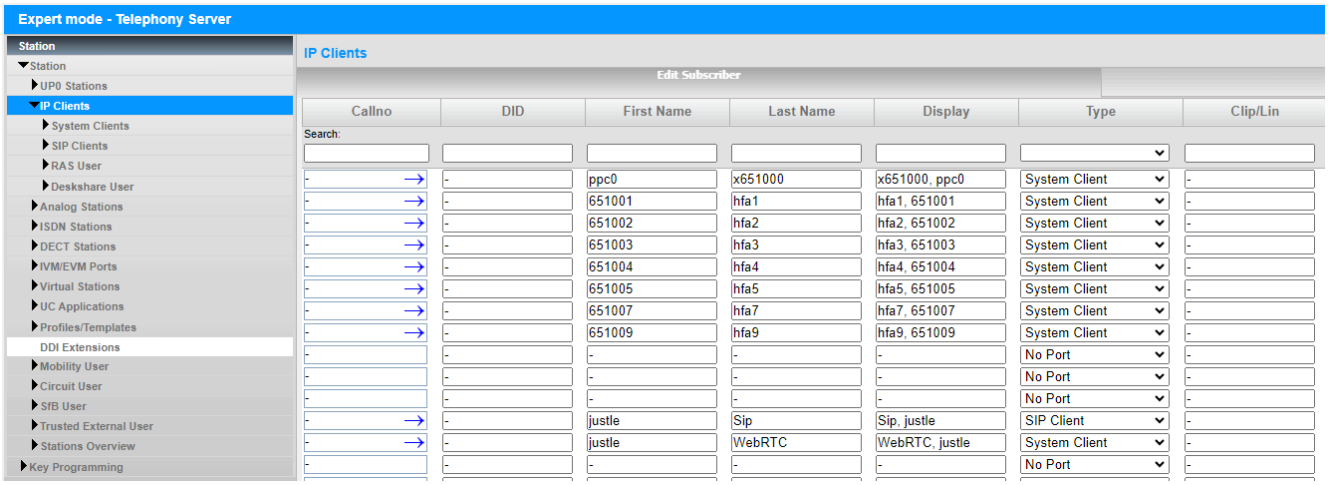
4) Once the SIP phone gets an IP and the DLI IP, the phone device will be registered into the DLI database, and a prompt will be displayed to enter the extension number.

5) Enter the terminal number on the phone (the number should be the same configured in the first step, e.g. 4111).

6) The reflash will start and the new HFA image will be downloaded to the phone. When the phone reboots it will be registered as an HFA phone and the plug and play data will be sent by the system towards the phone.

7) **To reflash an already registered SIP phone:**

8) Change the working SIP device type to "System Client".



9) Restart the phone.

10) The reflash will start and the new HFA image will be downloaded to the phone. When the phone reboots it will be registered as an HFA phone and the plug and play data will be sent by the system towards the phone.

7 Initial Setup of OpenScape Business UC Booster

This section describes the initial installation and configuration of the OpenScape Business UC Booster at the OpenScape Business X3/X5/X8 communication system. Note that a distinction is made here, depending on whether the OpenScape Business UC Booster Card or the OpenScape Business UC Booster Server is to be used for the UC Booster functionality.

The initial setup of the OpenScape Business UC Booster is carried out using the OpenScape Business Assistant administration program (web-based management, also called WBM in short).

The detailed administration of any features that are not covered by the initial setup is described in subsequent chapters.

Initial Setup of the OpenScape Business UC Booster Card

The OpenScape Business UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system and configured for operation. This is followed by the configuration of the OpenScape Business UC Booster functionality.

The specific installation steps required for the initial setup differ, depending on whether the UC Booster Card is being put into operation with the OpenScape Business X3/X5/X8 communication system for the first time or whether it is being integrated later in an existing and already configured OpenScape Business X3/X5/X8 communication system.

Overview of the installation steps for both options:

Integration in a New Communication System	Integration in an Existing Communication System
	Backing up the Configuration Data of the Communication System
Installing the UC Booster Card The UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system. For a description, see the OpenScape Business Service Documentation, Hardware Installation - Description of the Boards.	Installing the UC Booster Card The UC Booster Card is installed in the OpenScape Business X3/X5/X8 communication system. For a description, see the OpenScape Business Service Documentation, Hardware Installation - Description of the Boards.
Configuring the UC Booster Card The configuration of the UC Booster Card is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Integration into the Customer LAN.	Configuring the UC Booster Card The configuration of the UC Booster Card is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the Integration into the Customer LAN. For the specifics of the configuration, see Configuring the UC Booster Card

Integration in a New Communication System	Integration in an Existing Communication System
Basic Configuration The basic configuration is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Basic Configuration.	Basic Configuration The basic configuration is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the Basic Configuration. For the special features of the basic configuration, see Basic Configuration
Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Closing Activities.	Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Closing Activities. For the special features of the closing activities, see Closing Activities

Initial Installation of the OpenScape Business UC Booster Server

The OpenScape Business UC Booster Server is integrated together with the OpenScape Business X3/X5/X8 communication system in the customer LAN.

The OpenScape Business communication software for the OpenScape Business UC Booster Server, which provides the OpenScape Business UC Booster functionality, is installed on the Linux operating system SLES 12 SP5 64 bit or SLES 15 SP6 64-bit. The communication software can be operated directly on a Linux server or in a virtual environment with VMware vSphere. The installation of the Linux operating system is described in the installation guide *OpenScape Business, Installing the Linux Server*.

The OpenScape Business UC Booster Server has its own WBM. This WBM is used for software updates, backing up the configuration data and diagnostics of the OpenScape Business UC Booster Server. The initial installation of the OpenScape Business UC Booster server is performed with the WBM of the communication system.

The specific installation steps required for the initial installation differ, depending on whether the UC Booster Server is being put into operation with the OpenScape Business X3/X5/X8 communication system for the first time or whether it is being connected later to an existing and already configured OpenScape Business X3/X5/X8 communication system.

Overview of the installation steps for both options:

Integration in a New Communication System	Integration in an Existing Communication System
	Backing up the Configuration Data of the Communication System
Installing the Linux Server The installation of the Linux server is described in the OpenScape Business Linux Server Installation Guide.	Installing the Linux Server The installation of the Linux server is described in the OpenScape Business Linux Server Installation Guide.

Integration in a New Communication System	Integration in an Existing Communication System
Installing the Communication Software	Installing the Communication Software
Configuring the UC Booster Server The configuration of the UC Booster Server is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Integration into the Customer LAN.	Configuring the UC Booster Server The configuration of the UC Booster Server is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the Integration into the Customer LAN. For the specifics of the configuration, see Configuring the UC Booster Server
Basic Configuration The basic configuration is performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Basic Configuration.	Basic Configuration The basic configuration is performed later on an already configured OpenScape Business X3/X5/X8 communication system. For a description, see the Basic Configuration. For the special features of the basic configuration, see Basic Configuration
Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Closing Activities.	Closing Activities The closing activities (including the licensing of the UC Clients) are performed together with the initial installation of the OpenScape Business X3/X5/X8 communication system. For a description, see the Closing Activities. For the special features of the closing activities, see Closing Activities

7.1 Prerequisites for the Initial Setup

Meeting the requirements for the initial setup ensures the proper operation of the OpenScape Business UC Booster.

General

Depending on the used hardware (phones, ...) and the existing infrastructure, the following general conditions apply:

- The OpenScape Business X3/X5/X8 communication system is configured and ready for use.
- The LAN infrastructure (Internet routers, switches, etc.) is present and usable.
- The IP phones are connected to the customer LAN.
- A broadband Internet connection is recommended for software updates and remote access.
- All licenses required for the OpenScape Business UC Booster are present (e.g., UC clients, Directory Services, etc.). When integrating in an already licensed communication system, there is no activation period.
- An IP address scheme exists and is known.

- A dial plan (also called a numbering plan) is present and known.

For UC Booster Card

The following requirements must be observed for the operation of the UC Booster Card.

- OpenScape Business Hardware:

  The UC Booster Card is installed.
- Networking equipment:

  An IPv6-enabled networking equipment through which the UC Booster Card is connected with the communication system is mandatory for proper operation. This causes the UC Booster Card to automatically receive an IP address during the initial setup and after every restart of the system.

  If the networking equipment is not IPv6-enabled, the red LED of the communication system flashes. In this case, the Admin port of the system must be connected to the second LAN port of the UC Booster Card using an additional Ethernet cable. This causes the UC Booster Card to automatically receive an IPv4 IP address via the IPv6 protocol. As soon as the UC Booster Card is reachable over IP, the red LED of the communication system goes out. The desired IP address for the UC Booster Card can then be entered during the initial setup and after every restart of the system. Communication between the system and UC Booster Card now takes place through the IPv4 connection of the switch.

  NOTICE: The additional Ethernet cable should be left connected in case a restart or a reload is required.
- Fan kit:

  The UC Booster Card requires an additional fan. The fan kit depends on the communication system.
- Housing cover:

  For the OpenScape Business X3W, a new housing cover is required for the UC Booster Card fan kit.

  When migrating from HiPath 3000 systems, new housing covers to accommodate the UC Booster Card fan kit are required for OpenScape Business X3W/X5W and X3R/X5R.
- Communication software:

  The software of the communication system must be upgraded to the latest released software version. Note that the image including the UC Booster Card software must be used for this purpose.
- Web browsers:

  The Admin PC is used for the initial setup of the UC Booster Card with the OpenScape Business Assistant (WBM). The WBM is browser-based and is

thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.

The following HTML 5-enabled web browsers are supported:

– Microsoft Internet Explorer Version 10 and later.
– Microsoft Edge
– Mozilla Firefox Version 17 and later
– Google Chrome

If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.

NOTICE: Unrestricted network access is needed between OSCC and OCAB.

For UC server Booster

The following requirements must be observed for the operation of the UC Booster Server.

- Linux server:

  The Linux server required for OpenScape Business S was installed as per the instructions in the *OpenScape Business Linux Server Installation Guide*, was integrated into the customer LAN, and is ready for use.
- OpenScape Business communication software:

  The installation DVD with the OpenScape Business communication software is available. After the software installation, the software of the communication system and communication software of the UC Booster Server must be updated separately to the same, latest released software version.
- DVD or USB stick with Linux operating system SLES 12 SP5 64 bit or SLES 15 SP6 64-bit.

  The Linux DVD may be needed during the installation of the OpenScape Business communication software, since some software packages (RPM) required for the communication software may need to installed later from this DVD.
- Web browsers:

  For the initial setup of the UC Booster Server with the OpenScape Business Assistant (WBM), either the Linux server or the Admin PC can be used. The WBM is browser-based and is thus independent of the operating system. A screen resolution of 1024 x 768 or higher is required.

  The following HTML 5-enabled web browsers are supported:

  – Microsoft Internet Explorer Version 10 and later (Admin PC).
  – Microsoft Edge
  – Mozilla Firefox Version 17 and later (Linux server / Admin PC)
  – Google Chrome

  If an older version of the web browser is installed, you will need to install an up-to-date version before you can start the initial setup of the system.
- Firewall:

  When connected to the Internet, a firewall is needed for the Linux server to prevent unauthorized access from outside. After installing Linux, the Linux

firewall is enabled. The installer of the communication software adjusts the firewall settings so that the communication software can be operated properly. The ports for the communication software are opened, and all other ports are closed.

If an external firewall is used in the network, the Linux firewall must be disabled, and the addresses and ports required for the communication software must be opened (see Used Ports).

7.2 Backing up the Configuration Data of the Communication System

Before installing the OpenScape Business UC Booster, the existing configuration data of the OpenScape Business communication system must always be saved by creating a backup.

The backup is performed at the WBM of the OpenScape Business communication system.

It can be stored on different backup media (such as a USB drive or a network drive).

7.2.1 How to Perform a Data Backup

Prerequisites

You are logged in at the WBM of the communication system with the **Advanced** profile.

For a data backup on a USB device, the USB device must be connected to the USB server interface of the communication system.

Step by Step

1) Click on **Backup and Restore** in the navigation bar.
2) In the navigation tree, click **Backup - Immediate**.
3) Enter a comment for the backup set in the **Comment** field in the **Name** area so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) Activate the target drive on which the backup set is to be saved in the **Devices** area.
5) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.
6) The backup was successful if the message **Backup completed successfully!** appears. Click on **Finish**.
7) If you are using a USB stick as the backup medium, wait until the LED of the USB stick stops blinking. This ensures that the backup has been successfully saved on the USB stick. You can then safely remove the USB stick.
8) This completes the backup with the WBM. Exit the WBM by right-clicking the **Logout** link on the top right of the screen and then close the window.

7.3 Commissioning the UC Booster Card

The commissioning of the UC Booster Card includes the installation in the OpenScape Business communication system and the initial configuration for proper operation.

After completing the configuration successfully, a software update must be performed.

7.3.1 Installing the UC Booster Card

The UC Booster Card is integrated into the OpenScape Business communication system. The slot used for the UC Booster Card depends on the communication system.

The installation of the UC Booster Card is described in detail in the service documentation Hardware Installation under the section "Description of the Boards".

The UC Booster Card can be integrated into the following OpenScape Business communication systems:

- OpenScape Business X3R and X5R (OCCMR)

  UC Booster Card with additional fan kit.
- OpenScape Business X3W and X5W (OCCM)

  UC Booster Card with additional fan kit.

  For the OpenScape Business X3W, a new housing cover for the fan kit is also required.
- OpenScape Business X8 (OCCL)

  UC Booster Card with additional fan kit.

7.3.2 Configuring the UC Booster Card

During the configuration, the basic settings for the operation of UC Booster Card are set up.

The configuration of the UC Booster Card is performed with the **Initial Installation** wizard in the WBM of the communication system. The description of the configuration can be found in the section Initial installation of OpenScape Business X3/X5/X8.

The **Initial Installation** wizard of the WBM includes the initial configuration of the entire communication system. The following configuration components are important for the operation of the OpenScape Business UC Booster Card:

- IP address of the UC Booster Card

  The UC Booster Card requires a separate IP address from the network segment of the communication system.
- Selection of the UC solution

  You can select whether the UC solution UC Smart or UC Suite is to be used.

Changing the IP address of the UC Booster Card or UC solution leads to a restart of the communication system.

7.3.3 Updating the Software for the UC Booster Card

In order to enable the UC Booster Card to operate correctly, the software of the communication system needs to be updated. All missing software components for the UC Booster Card will then be installed.

If the software of the communication system is already up-to-date, the system must be updated again with the latest software to ensure that all components required for the UC Booster Card functionality are now installed.

The software update can be optionally performed via the Internet or via an image file, which can be obtained from the Software Download Server. When performing the update via the image file, make sure that the image file containing the UC Booster Card portions (osbiz..._ocab.tar) is used.

7.3.3.1 How to Perform a Software Update

Prerequisites

Access to the Internet is available.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) In the navigation tree, click on **Software Update** > **Update via Internet**. The currently installed software version is displayed to you.
3) Click on **OK & Next**.
4) Read the license agreement (EULA) fully and then enable the radio button **I accept the license agreement**.
5) Click on **OK & Next**.
6) Select the radio button **Start Action - Immediately / Immediately after transfer**.
7) Click on **OK & Next**. The software update is loaded into the communication system in the background and automatically activated after the transmission. After two restarts, the software is up-to-date.

   NOTICE: You can close the browser window at any time.

8) You can check the current status of the update with the WBM under **Service Center** > **Software Update** > **Status**.

7.4 Commissioning the UC Booster Server

The commissioning of the the UC Booster Server includes the installation of the OpenScape Business communication software on the Linux server and the initial configuration for proper operation.

After completing the configuration successfully, a software update must be performed.

7.4.1 Installing the Communication Software

The OpenScape Business communication software is installed on the Linux server using the OpenScape Business DVD.

Make sure that the IP addresses and network masks to be configured are appropriate for the customer LAN.

DHCP Server

A DHCP server automatically assigns a unique IP address to each IP station (IP phones, PCs, etc.) and provides the IP stations with network-specific data such as the IP address of the default gateway, for example.

Either an external DHCP server (e.g., the DHCP server of the Internet router or of the communication system) or the DHCP server of the Linux server can be used as a DHCP server. If the DHCP server of the Linux server is used, the external DHCP server must be disabled. The configuration of the Linux DHCP server can be performed during the installation of the OpenScape Business communication software.

Virtual Environment

The communication software can run in a virtual environment. To do this, the virtualization software (host operating system) must be first installed and configured on the server PC. Linux is then installed as a guest operating system. Within the Linux operating system, the communication software is installed last (see the *OpenScape Business Linux Server Installation Guide* for more details).

Use of snapshots on virtual machines (VM):

Snapshots can be a valuable maintenance mechanism, for example, to perform a fast rollback to a predefined operating state of the VM after a mass distribution script has failed.

- Snapshots cannot be created during normal operation. While a snapshot is being taken, the current operating state of the virtual machine is frozen. Consequently, connected devices and applications such as IP phones or the UC clients can lose the connection to the server.
- Snapshots can cause internal server processes to lose their synchronization, which means that the stable operation of the communication system can then no longer be guaranteed. A server reboot following the snapshot should therefore also be planned within the maintenance timeframe.
- Previous snapshots should not remain on the production environment during normal operation.
- Snapshots can be taken during a planned maintenance window or within the framework of the installation.
- Snapshots are used internally by backup tools such as VDP or VDR. It must be ensured that these backup operations are schedules outside of business hours and that the snapshots generated by these tools are deleted at the end of the operation.

More information regarding snapshots can be found the VMware knowledge base (KB). A good starting point is the KB article 1025279 – Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

7.4.1.1 How to Install the Communication Software

Prerequisites

- The SLES 12 SP5 or SLES 15 SP6 operating system has been correctly installed and started on the Linux server.
- DVD or .ISO file with OpenScape Business communication software.
- DVD or .ISO file or USB stick with the Linux operating system SLES 12 SP5 64-bit or SLES 15 SP6 64-bit, for any subsequent installation of software packages (RPM) that may be required.
- The root access data (user name and password) for logging into the Linux server is available.

IMPORTANT: The OpenScape Business communication software overwrites any existing configuration files (e.g., for DHCP, FTP, Postfix, etc.) during the installation.

Step by Step

1) Log into the Linux server with root privileges.

2) Insert the OpenScape Business DVD or .ISO file into the DVD drive.

3) Confirm the message with **Run**. The "Welcome" window appears.

4) Select the desired setup language (e.g., **English**) and click **Start**. The rest of the installation is described here for the English language.

5) Select the desired product from the list and click on **Select**. A check is performed to determine whether the hardware meets all the requirements for the installation. A warning is displayed for minor shortfalls in meeting the requirements. After confirmation, the installation can then be continued. For severe shortfalls, the installation is canceled automatically.

6) A check is performed to determine whether additional RPM packages need to be installed. If yes, confirm this with **Confirm**. If this occurs, you will need to switch back to SLES 12 or SLES 15, DVD or .ISO file later.

7) A window with the terms of the license (i.e., the End User License Agreement or EULA) appears. Read the terms of the license and accept the license agreement with **Yes**.

8) If a DHCP server is already present in the customer LAN (e.g., the DHCP server of the Internet router), stop the configuration of the Linux DHCP server here with **No** and proceed to step 12 to continue.

NOTICE: In order to ensure that the software of system telephones can be updated automatically even when using an external DHCP server, you have two options:

a) The IP address of the Linux server must be entered as the DLS address at each system telephone.

b) The network-specific data must be entered at the external DHCP server. The parameters for this can be found under `/var/log/OPTI.txt`.

---

9) If you want to use the Linux DHCP server, click on **Yes** to enable and configure the Linux DHCP server.

10) Enter the following values (preset with default values):
    - **Default Route**: IP address of the default gateway; as a rule, the IP address for the Internet router, e.g., `192.168.5.1`.
    - **Domain** (optional): the domain specified during the Linux installation, e.g., `<customer>.com`
    - **DNS-Server** (optional): IP address of the DNS server specified during the Linux installation. If no DNS server is available in the internal network, you can enter the IP address of the Internet router (e.g., `192.168.5.1`) here.
    - **SNTP Server**: IP address of the internal or external NTP server.
    - **DLS/DLI Server**: IP address of DLS server, i.e., the IP address of the Linux server (e.g.: `192.168.5.10`).
    - **Subnet**: appropriate subnet for the IP address range, e.g.: `192.168.5.0`.
    - **Netmask**: Subnet mask of the Linux server that was specified during the Linux installation, e.g.: `255.255.255.0`.
    - **IP range begin** and **IP range end**: IP address range from which the DHCP server may assign IP addresses, e.g.: `192.168.5.100` to `192.168.5.254`.
11) Click on **Continue**.
12) After the installation, the Linux operating system needs to be restarted. Select the check box **PC Reboot** and confirm with **Continue**.
13) If additional RPM packages need to be installed, you will be prompted to insert the SLES 12 DVD or SLES 15 USB stick. Insert the DVD or USB stick and confirm with **Continue**. Following the successful installation of the RPM packages, reinsert the OpenScape Business DVD or .ISO file and confirm this with **Continue**, followed by **Run**.
14) The OpenScape Business communication software is installed. The operating system then automatically performs a restart.
15) After the restart, log in with the user account that was set up earlier during the Linux installation.
16) Right-click on the DVD drive icon on the desktop and select the menu item **Eject**. Remove the OpenScape Business DVD from the DVD drive.

NOTICE: It takes a few minutes until all components of the OpenScape Business communication software are active.

7.4.2 Configuring the UC Booster Server

During the initial configuration, the basic settings for the operation of the UC Booster Server are defined.

The configuration of the UC Booster Server is performed with the **Initial Installation** wizard of the WBM of the communication system. A description of the configuration can be found in the section "Initial installation of OpenScape Business X".

The **Initial Installation** wizard of the WBM includes the initial configuration of the entire communication system. The following configuration components are important for the operation of the OpenScape Business UC Booster Server:

- Selection of the UC solution

  You can select whether the UC solution UC Smart or UC Suite is to be used. The IP address of the Linux server must be entered for this purpose.

  Changing the UC solution leads to a restart of the communication system.

In addition, the IP address of the communication system must be made known at the WBM of the UC Booster Server.

7.4.2.1 Announcing the IP Address of the Communication System

Prerequisites

The UC Booster Server is integrated in the customer LAN and operational.

The OpenScape Business communication system is operational.

Step by Step

1) Start the web browser on the Linux PC and invoke the WBM of the OpenScape Business server at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.1.10`

2) If the browser reports a problem with a security certificate, install the certificate (using the example of Internet Explorer V10).

a) Close the web browser.
b) Open the web browser with administrator rights by clicking the right mouse button on the web browser icon and selecting the menu item **Run as administrator** from the context menu.
c) Allow the User Account Control.
d) Open the WBM of the OpenScape Business server at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.1.10`

e) Click on **Continue to this website**.
f) Click on the message **Certificate Error** in the navigation bar of the web browser.
g) Click on **View Certificates**.
h) Click on **Install Certificate** (only visible with administrator rights).
i) Select the option **Local Computer** and confirm with **Next**.
j) Select the option **Place all certificates in the following store**, click **Browse** and specify **Trusted Root Certification Authorities**.
k) Confirm with **OK** and then with **Next** and **Finish**.
l) Confirm the certificate import with **OK** and close the certificate window **OK**.
m) Close the web browser.
n) Start the web browser again (without administrator rights) and invoke the WBM of the OpenScape Business sever at the following address:

`https://<IP address of the Linux server>`, e.g., `https://192.168.1.10`

3) Click on the language code at the top right and select the language in which the user interface of the WBM is to be displayed from the menu. The Login page will be displayed in the selected language.
4) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> **NOTICE:** If you go to the **Password** field after entering `administrator`, `@system` will be added automatically.

5) In the second field under **Login**, enter the dStart the web browser on the Linux PC and invoke the WBM of the OpenScapeefault password `administrator` for access as an administrator.
6) Click **Login**.
7) The following steps are only required once when first logging on to the WBM:
   a) Reenter the default password **administrator** in the `Password` field.
   b) Enter a new password in the **New Password** and **Confirm New Password** fields to protect the system against misuse. Note case usage and the status of the `Num` und `CapsLock` keys. The password is displayed as a string of asterisks (*).

> **NOTICE:** The password must be at least 8 characters long and include a digit. Make sure that you remember your new password.

   c) Click **Login**.
   d) Select the current date and enter the correct time.
   e) Click **OK & Next**. You are automatically logged out of the WBM.
   f) In the field under **Login**, enter the default user name `administrator@system` for access as an administrator.

> **NOTICE:** If you go to the **Password** field after entering `administrator`, `@system` will be added automatically.

   g) In the second field under **Login**, enter your new password for access as an administrator.
   h) Click **Login**. The home page of the WBM appears.
   i) Click on **Administrators** in the navigation bar.
   j) In the **Administrators List**, select the check box before the list item **Administrator**.
   k) Click **Edit**.
   l) In the **User role** drop-down list, select the user profile **Expert**.
   m) Click **OK & Next**.
   n) Log out from the WBM via the **Log Out** link at the top right.
   o) Log into the WBM again with the default user name `administrator@system` and the newly defined password.
8) In the navigation bar, click on **Expert Mode**.
9) Click **Maintenance** > **Configuration** in the navigation tree.
10) On the **Change Gateway IP Address** tab, under **Gateway IP Address**, enter the IP address of the communication system (e.g., `192.168.1.2`).
11) Click **Apply**.

7.4.3 Updating the Software for the UC Booster Server

In order to ensure that the UC Booster Server operates correctly, the software of the communication system and the communication software of the UC Booster Server must be updated to the same software level.

If the software of the communication system is already up-to-date, only the software of the UC Booster Server needs to be updated.

The software update can be optionally performed via the Internet or via an image file, which can be obtained from the Software Download Server. When updating the UC Booster Server via the image file, make sure that the image file containing the UC Booster Server portions (osbiz..._pcx.tar) is used.

7.5 Basic Configuration

During the basic configuration, the most important settings for the operation of the OpenScape Business UC Booster are defined.

The basic configuration for both the UC Booster Card and the UC Booster Server are performed by using the **Basic Installation** wizard of the WBM of the communication system. A description of the basic configuration can be found in the section Initial Installation of OpenScape Business X.

The basic configuration covers the configuration of the entire communication system. The following configuration items are important for the operation of the OpenScape Business UC Booster:

- Station data

  Special phone numbers required for the operation of the OpenScape Business UC Booster can be adapted as required. For example, the call number of the UC Suite voicemail box must be specified here.
- Configuring the UC Booster Card

  If a UC Booster Card is integrated in the communication system, the automatic configuration of the UC Booster Card must be initiated.
- Meet-Me conference settings

  The Meet-Me conference feature is available with OpenScape Business UC Booster. The pre-assigned call number and the pre-assigned dial-in number for the Meet-Me conference can be changed.

7.6 Closing Activities

After the initial installation and the basic installation with the WBM have been completed, some important settings must still be made for the operation of the OpenScape Business UC Booster.

The closing activities for both the UC Booster Card and the UC Booster Server are performed with the WBM of the communication system. A description of the closing activities can be found in the online help or in the OpenScape Business Administrator Documentation under the section "Initial Installation of OpenScape Business X".

The following closing activities are important for the operation of the OpenScape Business UC Booster:

- Activate and assign licenses

  If the OpenScape Business UC Booster is being integrated in an already licensed communication system, the licenses must be activated immediately in order to use its functionality. If the OpenScape Business UC Booster is being integrated in a communication system that has not yet been licensed, the licenses must be activated within a period of 30 days. Once the licenses have been activated successfully, they must be assigned to the stations. In a standalone system, system-wide features are enabled automatically upon activation.
- Provision the UC Clients for installation

  The UC clients are part of the UC Suite. The installation files for the UC Client are accessible via the WBM and can be made available to the IP stations automatically or manually.
- Perform a data backup

  All previous changes to OpenScape Business must be backed up. The backup can be stored as a backup set on a USB storage device or on the internal network.

  For the UC Booster Card, it is sufficient to perform a backup of the communication system. For the UC Booster Server, the data of the communication system and the data of the communication software of the UC Booster Server must be backed up separately.

7.7 Uninstalling the Communication Software

The software communication can be uninstalled via a text console.

7.7.1 How to Uninstall the Communication Software

Step by Step

1) Open a terminal (e.g., a GNOME terminal).

2) Enter the command `su` (for superuser = root) in the shell interface and confirm it by pressing the Enter key.

3) Enter the password for the "root" user in the shell interface and confirm it by pressing the Enter key.

4) Enter the command `oso_deinstall.sh` in the shell interface and confirm it by pressing the Enter key. Follow the instructions of the uninstallation program.

7.8 Upgrading from the UC Booster Card to the UC Booster Server

In order to upgrade an OpenScape Business communication system with an integrated UC Booster Card to an OpenScape Business communication system with a connected UC Booster Server, the following steps must be performed as described below:

Upgrade Steps

Perform the following steps in sequence:

1) **Back up the configuration data**

   Perform a backup of the configuration data of the communication system.

   For a description of the backup procedure, see Backing up the Configuration Data of the Communication System.

2) **Change the IP address of the UC Booster Card**

   Using the **Initial Installation** wizard in the WBM of the communication system, change the IP address of the UC Booster Card to an unused IP address. The UC clients will be disconnected.

   For a description of how to change the IP address, see System Settings .

3) **Change the application selection**

   Using the **Initial Installation** wizard in the WBM of the communication system, change the application selection from **Package with UC Suite** to **Package with UC Suite on OSBiz UC Booster Server** if you are using UC Suite (or from **Package with UC Smart** to **Package with UC Smart on OSBiz UC Booster Server** if you are using UC Smart) and enter the former IP address of the UC Booster Card as the IP address of the UC Booster Server.

   For a description of the application selection, see UC Solution.

4) **Installing the Linux Server**

   The Linux operating system approved for the UC Booster Server must be installed on the Linux server.

   A description of the Linux installation can be found in the OpenScape Business Linux Server Installation Guide.

5) **Change the IP address of the UC Booster Server.**

   The former IP address of the UC Booster Card must be specified as the IP address of the UC Booster Server (= IP address of the Linux server). You can enter the IP address of the Linux server during the installation of the Linux operating system or change this later using YaST.

   For a description of IP address assignment during the Linux installation, see the OpenScape Business Linux Server Installation Guide.

6) **Install the communication software**

   The OpenScape Business communication software must be installed on the Linux server.

   For a description of the installation of the communication software, see Installing the Communication Software.

7) **Configuring the UC Booster Server**

   Enter the IP address of the communication system in the WBM of the UC Booster Server.

   For a description of IP address assignment of the communication system, see Configuring the UC Booster Server.

8) **Restart the communication software**

   Restart the UC Booster Server communication software via the WBM of the UC Booster Server.

   For a description of the restart, see Restarting the UC Application .

9) **Update the software**

The software of the communication system and the UC Booster Server must be updated to the same software level.

For a description of the software update, see Updates.

10) **Restore the configuration data**

Restore the backed up configuration data of the communication system in the WBM of the communication system. The communication system and the communication software are subsequently restarted, and the connections to the UC Suite clients are restored.

For a description of how to restore data, see Restore .

7.9 Used Ports

The OpenScape Business system components use different ports, which may need to be opened in the firewall as required. For the ports of the web-based clients (e.g., myPortal to go), port forwarding must be configured in the router.

An actual and complete list of all used ports of OpenScape Business is available in the "Interface Management Database" (IFMD) which can be accessed via the Partner Portal of Unify (https://unify.com/en/partners/partner-portal.

NOTICE: The ports identified with "O" in the list below are optional, i.e., are not permanently open in the firewall.

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
System components							
Admin Portal (https)	X		443	X	X	X	X
CAR Alive checks	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (up to V3R3) 7780, 7791 (V3R3.1 and higher)	O		O	
Communication Client Installer	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

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (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			
LDAP server	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
OpenScape Business status server	X		8808	X		X	X
OpenScape Business user portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (embedded)		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	

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
SNMP (traps)		X	162	X		X	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Web-based clients							
Web-based clients (http)	X		8801	X	X	X	X
Web-based clients (https)	X		8802	X	X	X	X

NOTICE: For security reasons, we recommend that only https be used for the web-based clients and that port forwarding be set up from external TCP/443 to internal TCP/8802.

CLS certificate

Starting with V3R3.1, a new CLS certificate with an updated Common Name (CN) is provided via a newly introduced port. This offers an improved and stronger digest algorithm as well as updated legal entities. Systems licensed online via CLS Connect mode, require the following two prerequisites:

- The IP address 188.64.16.4 is enabled for outgoing traffic in the firewall.
- Ports 7780 and 7791 are enabled for outgoing traffic in the firewall.

The previously used port 7790 can be removed from the firewall configuration after the upgrade to V3R3.1 to increase security.

8 Licensing

The flexible licensing concept of OpenScape Business allows customers to adapt the functional scope to their own requirements through licenses. All OpenScape Business X and OpenScape Business S communication systems are subject to this license concept. Phones, UC clients, UC functions and system-wide features can thus be unlocked according to individual customer needs. Uniform licenses are used for all OpenScape Business communication systems.

OpenScape Business can be expanded or equipped with additional features at a later date by purchasing additional licenses.

All licenses are always bound to the basic license of the communication system and enable the use of the purchased features for the associated version of OpenScape Business.

90-day evaluation licenses can be ordered to allow customers to test and evaluate special features.

NOTICE: It is advisable not to install license files or run any wizard if the system is live, as active calls may be dropped.

Activation Period

The license activation must be completed within the activation period (duration of 30 days). The activation period begins when the current date is entered in the WBM. The expiration date of the activation period is stored in the process.

During the activation period, the product is fully functional, and the maximum number of licenses are available for use.

If the system loses the current date within the activation period (e.g., due to a discharged battery on the mainboard), the date must be updated in the WBM as soon as possible so that the system can continue to be used without restrictions during the activation period.

If the licensing is not completed before the activation period expires, the functionality of the communication system will be severely restricted. Internal communication between the individual stations is still possible, but only the first two active phones can make external calls (e.g., for emergency calls). Access to the communication system via Remote Access is still possible. The system also remains in this restricted state when the initial installation is carried out only with Manager E, since this does not start the activation period.

License Structure

The licenses for the communication system are structured as follows:

- A basic license permanently activates the software of the communication system. This basic license is also required for activating all other licenses.
- Station licenses activate the phones for external voice communications.
- User-oriented licenses to unlock specific user features.
- System licenses to unlock general system-wide features.

Migration

Existing HiPath 3000 V9 customers are being offered an upgrade license for license migration. License migration ensures investment protection for customers through continued use of telephones and voice features.

NOTICE: For information regarding licensing and upgrating or migrating systems in a network, please see **Network - Licensing** section in Updates chapter.

Related concepts

Stations on page 406

8.1 Licensing Procedure

Licensing is handled via the centralized OpenScape License Management procedure for the administration and activation of licenses. This ensures that a customer can use precisely the system configuration or features for which that customer has acquired the appropriate licenses (usage rights).

The licenses of the OpenScape Business communication systems are bound to the Locking ID or the Advanced Locking ID of the communication system (see Locking ID and Advanced ID Locking).

The customer orders the required features and receives a License Activation Code (LAC). After a successful initial installation of the communication system, the customer activates the acquired licenses via a license file. The license file provides the system with a license pool with all purchased licenses available for the subsequent allocation of licenses.

The WBM provides wizard-driven functions for the customer registration, license activation and the license assignments for standalone systems and systems in an OpenScape Business internetwork. Licensing with Manager E is not possible.

Steps for Successful Licensing

1) Configuration of the system within the activation period
2) Registration of customer data
3) License Activation
4) Assigning Licenses

Customer Registration

Within the framework of licensing, the input of the customer data of each respective system is mandatory for the registration of the customer. The customer data is used to retrieve information quickly in the case of security-related issues, especially in the context of product recalls. In addition, customers receive information on prevention of license misuse by third parties, e.g., via the new link to the license information.

License Activation

During the license activation, the purchased licenses are bound to the communication system using the license management of the WBM. Two methods are available for this:

- Online activation

  For online activation, after the LAC is entered via the Internet, a connection to the Central License Server (CLS) is set up, and the license file is automatically transferred to the integrated license agent (Customer License Agent, CLA) in the communication system. The licenses are then automatically activated.
- Offline activation

  With offline activation, the communication system is not connected to the Central License Server (CLS). The license file is generated at the CLS by an authorized partner and must be transmitted manually during the license activation to the integrated license agent (Customer License Agent, CLA) in the communication system.

Assigning Licenses

All purchased licenses are permanently assigned to stations via the license management of the WBM.

To assign licenses to stations, the stations must be first set up with the WBM, e.g., during the initial installation. Each system configuration can be set independently of the existing licenses. However, the corresponding feature can only be used once the license have been assigned.

When assigning licenses, a distinction is made between the configuration and actual licensing. For station and user-oriented licenses, licence requests are first configured. If a license is available in the license pool for a license request, the corresponding feature is unlocked. If no license is available in the license pool, the configured license request is retained, but the corresponding feature is not unlocked. Missing licenses must be purchased if needed.

Licensing in an Internetwork

For an OpenScape Business internetwork, a network-wide license file (network license file) is generated by an authorized partner at the Central License Server (CLS). This network-wide license file is managed by the Central License Agent (CLA) of the master node and provides the licenses for the individual nodes. The assignment of the licenses occurs via the WBM of each individual node. Within an internetwork, the network licenses can be shifted freely by using the WBM.

Online activation is not possible when licensing an internetwork.

Pay As You Go

Apart from the traditional licensing scheme, OpenScape Business supports subscription licensing model (Pay As You Go). "Pay As You Go" gives the opportunity to invoice only for the used licenses on each billing period and use extra licenses without extending the license file. There is no need to decide the amount of the licenses beforehand

A permanent internet connection from OpenScape Business system to the Central License Server (CLS) is required. It can be activated either online with a a License Activation Code (LAC) or with file upload. After installing, configuring the solution according to the custom needs and activating "Pay As You Go" a periodically report of the used licenses are sent to the Central License Server (CLS) and is evaluated. Once a month, a final report is created on the Central License Server (CLS) product site and the content of used licenses of this final report is used for license accounting.

With subscription licensing a new time period is introduced, the qualifying period. The qualifying period starts with the system startup or if a "Pay As You Go" license file is activated. The period starts consecutively and during this period a license configuration done in WBM will not lead to license usage update. The maximum duration of the qualifuing period is 2 hours.

NOTICE: In order the firewall to have access to CLS the following actions are needed:-

- 7790 port for outgoing IP traffic released

- 188.64.16.4 released for outgoing IP traffic

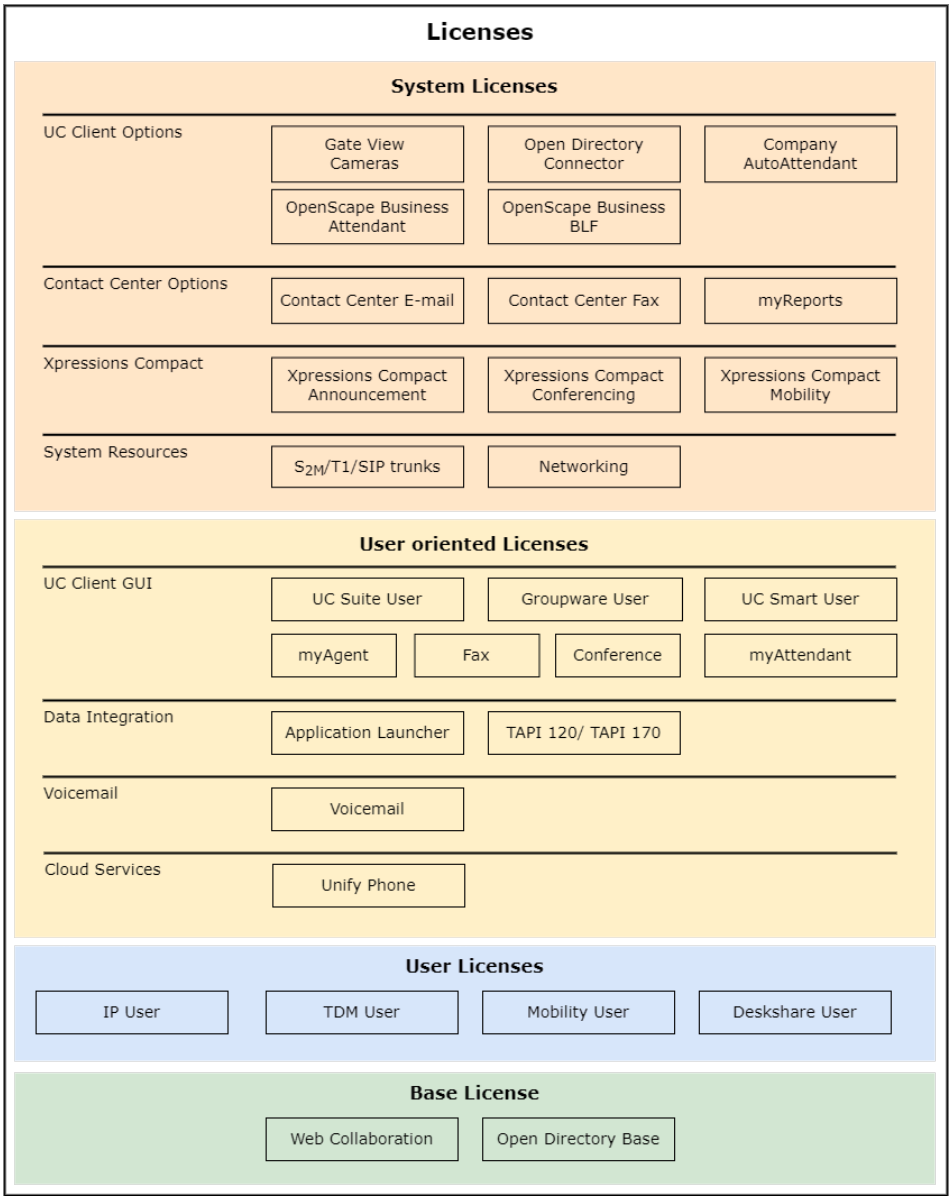
Newer V3R3 software systems utilize port 7791 for online license activation.

8.2 Licenses

To use the features of the communication system, licenses must be purchased. The purchased licenses must be activated within a given period of time (activation period).

Licenses are categorized thematically into license groups. The following license groups are available:

- Basic Licenses
- Station Licenses
- User-oriented Licenses
- System licenses



The above licenses can be used for OpenScape Business X, OpenScape Business S and the OpenScape Business UC Booster Server. There is no basic license for the UC Booster Server. The licenses cover all features and can be combined in accordance with the wishes of the customer. The possible combinations of licenses are explained in greater detail in the "Assigning Licenses and License Profiles" section.

Station licenses and user-oriented licenses are permanently assigned to subscribers.

8.2.1 Basic License

A basic license permits the basic use of the communication system. It is also required for activating all other licenses.

Internet telephony and emergency operation is also possible without a basic license.

The following basic licenses are available:

- **OpenScape Business V2 X1 Base**

  for unlocking the V2 functionality of

  – OpenScape Business X1

  The basic license additionally includes the licenses OpenDirectory Base for using the Open Directory Service (ODS) and Web Collaboration for starting a web collaboration session. This makes it possible for the UC solution UC Smart to be connected to an external database.
- **OpenScape Business V2 Base**

  for unlocking the V2 functionality of

  – OpenScape Business X3/X5/X8 with or without UC Booster (UC Booster Card or UC Booster Server) or
  – OpenScape Business S

  The basic license additionally includes the license OpenDirectory Base for using the Open Directory Service (ODS) and Web Collaboration for starting a web collaboration session. This makes it possible to connect the UC solutions UC Suite or UC Smart to an external database.

8.2.2 User Licenses

Every subscriber connected to the communication system requires a user license to make external calls. This license is permanently bound to the call number of the subscriber via the WBM.

User licenses include the comprehensive voice functionality of OpenScape Business. Additional licenses are required to use the UC solutions UC Smart or UC Suite (see User-oriented Licenses).

The following station licenses are available:

- **IP User**

  For the use of IP system telephones (HFA) and SIP telephones.
- **TDM User**

  For the use of UP0 system phones, analog phones, analog fax devices, ISDN phones, ISDN fax and DECT phones.
- **Mobility User**

  For the use of GSM/mobile phones, smartphones and tablet PCs as an extension of the communication system. For the use of myPortal to go and Mobility Entry. The assignment of an additional desk phone is not required. For the use of the Unify Phone client in combination with OpenScape Business.
- **DeskShare User**

  For use of the DeskSharing feature. Only a phone number and no physical phone is permanently assigned to such users. DeskShare users can operate specific IP system phones using their permanently assigned phone number, and they can access their personal phone settings on these phones.
- **Fallback User**

  For basic telephony use in case of an event of failure of a system node. The license is supported as a time based Pay As You Go license. So, the usage

time is calculated based on the days the system is hosting users from other nodes. The licenses are only effective during this hosting time. In a normal operation mode fallback users are like unlicensed users.

Flexible User Licensing

With the flexible user licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM, DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

The use of flexible user licensing requires the software version V1R3.3 and a newly generated license file at the CLS, which must be imported into the OpenScape Business and activated.

UC-Suite Flexible User Licensing

With the UC-Suite flexible user licensing, myPortal for Desktop users can also be licensed with myPortal for Outlook user licenses. If all the acquired myPortal for Desktop licenses have already been assigned, and further users are required, then the myPortal for Outlook User licenses can be used to meet this demand.

The use of flexible user licensing requires the software version V2 and a newly generated license file at the CLS, which must be imported into the OpenScape Business and activated.

8.2.3 User-oriented Licenses

User-oriented licenses are station-based and authorize the use of unified communications features and data integration applications. A user-oriented license also requires a station license and is permanently assigned to the phone number of the subscriber.

The following user-oriented licenses are available:

Voicemail

- **Voicemail**

  For the use of a personal voicemail box via the telephone (TUI) and via the user interface of the UC solutions UC Smart or UC Suite.

  NOTICE: If the UC solution UC Smart is expanded to UC Suite, the existing voicemail licenses and the assignments to the stations are retained.

  NOTICE: When assigning a VoiceMail license to an extension, a UC Suite user is created and all active call forwardings are reset.

Cloud Services

- **Unify Phone**

  For the use of the Unify Phone client in combination with OpenScape Business.

UC Client User Interface

- **UC Smart User**

  For the use of UC Smart functions of the communication clients myPortal @work, myPortal to go and other Web Services clients.
- **UC Suite User**

  For the use of UC Suite functions of the communications clients myPortal @work, myPortal for Desktop, myPortal to go and other Web Services clients.
- **Groupware user**

  For the use of UC Suite functions of the communications clients myPortal @work, myPortal for Outlook, myPortal to go and other Web Services clients.
- **Fax**

  For use of a fax box within the UC Suite. As a prerequisite, one UC User or Groupware User license is required additionally.
- **Conference**

  For the use of the UC Suite conference management features, such as managing and initiating permanent and recurring conferences. As a prerequisite, one UC User license or Groupware User license is required additionally.

  No license is required for participating in conferences.
- **myAttendant**

  For use of the UC Suite Attendant features.
- **myAgent**

  For the use of Contact Center functions such as information about queues, pop-ups with customer information on incoming calls, and access to the call history.

NOTICE: For the mobile client myPortal to go, besides the Mobility User license, an additional UC User license or Groupware User license is required for the UC solution UC Smart or for the UC solution UC Suite.

Data Integration

- **Application Launcher**

  For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information. Application Launcher can be operated with UC Smart, UC Suite or myAgent and additionally requires a UC User / Groupware User license or a myAgent license. It can optionally use the Open Directory Service.

- **OpenScape Business TAPI**

  For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors. The UC Booster (UC Booster Card or UC Booster Server) is a prerequisite.

8.2.4 System Licenses

System licenses are not subscriber-specific and unlock the system-wide features. These features can be used by all subscribers of the communication system.

Overview of system license requirements

Trunktype	SSP license	Trunk licesens/ channel	Networking license
ITSP	yes	yes	no
Native SIP trunk	yes	no	yes
Skype for Business	yes	yes	no
Unify Phone	yes	no	no
SIPQ-Interconnection	no	no	yes

The following system licenses are available:

System Resources

- **S_{2M}/T1/SIP trunks**

  For the use of S_{2M}/T1 and ITSP channels. S_0 channels do not need to be licensed. This also includes connections to S_0 Fax servers in PP mode.
  For the primary multiplex connections S_{2M} or T1 (USA), the individual voice channels are licensed. For ITSP connections, the number of simultaneous connections to one or more ITSP providers (SIP providers) is licensed. The number of possible simultaneous connections depends on the bandwidth of the connection.
- **Networking**

  For IP networking via SIP-Q/native SIP and/or TDM networking via CorNet-NQ or QSIG. For networking the UC Suite applications. One license is required per node.

  NOTICE: The networking license unlocks the lines for voice networking and UC Suite networking for a node. No S_{2M}/T1/ SIP trunk licenses are required for network trunks.

Table 3: Overview of System Resource Licenses (S_{2M}/ITSP)

Protocol	Licenses			
	No licence	OpenScape Business Networking (1x per system)	OpenScape Business S_{2M} / ITSP (1x per channel)	TDM User
S_0 internal				
Fax Server (DSS1/QSIG)	X			
Euro bus				per S_0 station
S_0 - CO trunks				
EURO CO PP	X			
Euro CO PMP	X			
S_{2M} - CO trunks				
EURO CO PP			X	
ITSP - Provider				
ITSP 1 to 8			X	
S_0 networking				
QSIG		X		
CorNet-NQ		X		
S_{2M} - Networking				
QSIG-Network		X		
CorNet-NQ		X		
SIP Networking				
SIP-Q		X		
native SIP		X		

Contact Center Options

- **Contact Center Mail**

  For setting up one or more email boxes to send and receive emails for Contact Center agents. A station license and a myAgent license are required for this. One license is required per node.
- **Contact Center Fax**

  For setting up one or more fax boxes to send and receive faxes for Contact Center agents. A station license and a myAgent license are required for this. One license is required per node.
- **myReports**

  For the compilation of statistics on the utilization of Contact Center resources based on different criteria. Using the Schedule Manager, reports can be created from over 100 predefined report templates for telephone, email and fax contacts. The report templates are managed via the Report Manager,

with functions for regrouping as well as adding and deleting newly created report templates.

UC Client Options

- **Open Directory Connector**

  For connecting to the Open Directory Service (ODS) in order to enable access to an external database or an external directory A maximum of four databases can be connected per node.
- **Company AutoAttendant**

  For the use of a central UC Smart or UC Suite based AutoAttendant to automatically transfer calls. One license is required per node.

  Announcements of the type "music on hold" (endless loop) are only played with this license.
- **OpenScape Business Attendant**

  For using the OpenScape Business Attendant (PC attendant). Up to 8 OpenScape Business Attendants may be licensed per node.

  If OpenScape Business Attendant should also have access to presence information, a UC User license is additionally required.
- **OpenScape Business BLF**

  For use of the additional Busy Lamp Field indicator of OpenScape Business BLF. For each subscriber, one BLF license and one UC User license is required. Up to 50 OpenScape Business BLFs may be licensed per node.

8.2.5 Evaluation Licenses

An evaluation license can be used to test special features with full functionality over a fixed time period (called the evaluation period) free of charge. If a regular license for the feature is activated during the evaluation period, the evaluation license will be disabled.

The following evaluation licenses are available:

- **OpenScape Business V3 Service Evaluation**

  This evaluation license is intended for partners who want to first preconfigure the communication system in their own company and put it into service at the customer site later. The 30-day activation period begins during the preconfiguration. In order to restart the activation period of 30 days after commissioning the system, this evaluation license must be activated from the customer site after starting up the system.

  The activation is possible once per system and only within the activation period. If the activation period has expired, the system must be licensed with permanent licenses.

  NOTICE: When Service Evaluation is activated CLS connect cannot be activated.

- **OpenScape Business V3 UC Smart Evaluation**

  This evaluation license is intended for customers who want to test the UC features of UC Smart. All UC Smart features can be used with this evaluation license.

  NOTICE: This evaluation license cannot be used if the communication system is located in an internetwork and the "Networking" license is active. If voicemail licenses are already available, they are used in combination with the new UC evaluation licenses.

- **OpenScape UC Suite V3 Business Evaluation**

  This evaluation license is intended for customers who want to test the UC features of UC Suite. All UC Suite features can be used with this evaluation license.

  NOTICE: This evaluation license cannot be used if the communication system is located in an internetwork and the "Networking" license is active. If voicemail licenses are already available, they are used in combination with the new UC evaluation licenses.

- **OpenScape Business V3 UC Suite Contact Center Evaluation**

  This evaluation license is intended for customers who want to test the Multimedia Contact Center. All features of the Multimedia Contact Centers can be used with the evaluation license.

  NOTICE: If the Multimedia Contact Center is not licensed within the evaluation period, the administrator must undo the Contact Center settings (e.g., delete schedules and queues, deactivate agents, etc.) before the evaluation license expires. Otherwise, errors may occur in OpenScape Business.

- **OpenScape Business V3 CRM Evaluation**

  This evaluation license is intended for customers who want to test Application Launcher, Open Directory Service and TAPI.

- **OpenScape Business V3 Attendant Evaluation**

  This evaluation license is intended for customers who want to test the OpenScape Business Attendant application.

- **OpenScape Business V3 BLF Evaluation**

  This evaluation license is intended for customers who want to test the OpenScape Business BLF application (e.g., to independently display the busy lamp field and presence information).

Rules

- The activation of an evaluation license occurs at the Customer License Server (CLS) and can only be performed once.
- The evaluation period is 90 days. After 60 days, the remaining time in days is counted backwards on the display of system telephones.
- When the evaluation period expires, the feature is automatically disabled.

- Multiple evaluation licenses may be active simultaneously in the system, but may then end at different times.
- If a perpetual license is active, the evaluation license is not started or, if already present, is stopped.

8.2.6 Upgrade Licenses

Upgrade licenses are required to upgrade HiPath 3000 V9, OpenScape Office V3 and OpenScape Business V1 systems to OpenScape Business V2 systems.

The license migration of HiPath 3000 systems requires a running and possibly licensed HiPath 3000 V9 system. The steps for the hardware and license migration must be carefully observed (see also the Migration). Pure HiPath 3000 TDM systems without licenses must be first upgraded to Version 9 and can then be migrated to OpenScape Business with an upgrade license.

The following upgrade licenses are available:

- **HiPath 3000 V9 Upgrade to OpenScape Business V2**

  For the migration from HiPath 3000 V9 to OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V8 Upgrade to OpenScape Business V2**

  For the migration from HiPath 3000 V8 to HiPath 3000 V9 and then to OpenScape Business V2 X3/X5/X8.
- **HiPath 3000 V7 Upgrade to OpenScape Business V2**

  For the migration from HiPath 3000 V7 to HiPath 3000 V9 and then to OpenScape Business V2 X3/X5/X8.
- **OpenScape Office V3 MX/LX Upgrade to OpenScape Business V2**

  For the migration from OpenScape Office V3 MX/LX to OpenScape Business V2.

8.2.7 Possible License Combinations

The licenses can be combined as desired. This section contains some suggestions for possible license combinations that will allow you to use the desired functions.

Please note that multiple licenses are required for some functions.

Telephony

- Required: IP User, TDM User or DeskShare User station license

---

NOTICE: Without a valid license, the phone can only be used for internal connections.

Telephony with UC Smart

- Telephony with voicemail box (UC Smart)
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented VoiceMail license

- Telephony with Mobility Entry (DISA-based mobility)
  - Required: Mobility User station license
- Telephony with myPortal to go
  - Required: Mobility User station license

    No Mobility User license is required in the **Desk phone** (control of the Office telephone) mode.
  - Required: user-oriented UC User license
  - Optional: user-oriented VoiceMail license
- Telephony with myPortal @work
  - Required: IP User
  - Required: user-oriented UC User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Conference license
- Telephony with myPortal @work VoIP
  - Required: IP User
  - Required: user-oriented UC User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Conference license
- Telephony with optiClient Attendant
  - Required: IP User, TDM User or DeskShare User station license
  - Required: OpenScape Business Attendant system license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented UC User license (for displaying the presence status)

Telephony with UC Suite

- Telephony with voicemail box (UC suite)
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented VoiceMail license
- Telephony with myPortal for Desktop
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented UC User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Fax license
  - Optional: user-oriented Conference license
- Telephony with myPortal for Outlook
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented Groupware User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Fax license
  - Optional: user-oriented Conference license

- Telephony with myPortal to go
  - Required: Mobility User station license

    No Mobility User license is required in the **Desk phone** (control of the Office telephone) mode.
  - Required: user-oriented Groupware User license or UC User license
  - Optional: user-oriented VoiceMail license
- Telephony with myPortal @work
  - Required: IP User
  - Required: user-oriented Groupware User license or UC User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Conference license
- Telephony with myPortal @work VoIP
  - Required: IP User
  - Required: user-oriented Groupware User license or UC User license
  - Optional: user-oriented VoiceMail license
  - Optional: user-oriented Conference license
- Telephony with myAttendant
  - Required: IP User, TDM User or DeskShare User station license
  - Required: user-oriented myAttendant license
  - Optional: user-oriented VoiceMail license

Telephony with Unify Phone

- Required: IP User
- Required: user-oriented Unify Phone license
- Optional: user-oriented VoiceMail license and additional IP User license for the team configuration

Using the Contact Center

- Required: IP User, TDM User, DeskShare User or Mobility User station license
- Required: user-oriented myAgent license

  At least one myAgent license must be active for the system to route and address Contact Center calls.
- Optional: Contact Center Email system license
- Optional: Contact Center Fax system license
- Optional: myReports system license

Using the Company AutoAttendant

- Required: Company AutoAttendant system license

  The Company AutoAttendant system license must be active for the system to route and address Auto Attendant calls.

8.3 Licensing a Communication System (Standalone)

The licensing of a standalone system must be performed in a specific order. This order is given in our example for one of the OpenScape Business X communication systems.

The following subsections describe how Step 3 and Step 4 can be performed using the WBM.

1) **License Authorization Code (LAC)**

   On purchasing licenses, the customer receives a License Authorization Code (LAC). The information on the licenses purchased are stored in the database of the Central License Server (CLS).

2) **Installation and Configuration**

   The customer or service technician uses the WBM wizard to install and configure the communication system (including the stations and lines). When you first launch the WBM, you must enter the current date. This starts the activation period (i.e., the period of 30 days during which the licensing has to be completed).

3) **License Activation**

   The customer or service technician uses the WBM to activate the licenses either online using a License Authorization Code (online license activation) or offline using a license file (offline license activation).

4) **Assigning Licenses**

   The customer or service technician uses the WBM to assign the purchased licenses to stations and lines. Once the licenses have been assigned successfully, the licensed features are activated.

8.3.1 CLS Connect

CLS connect allows you to make unlimited rehosts of your OpenScape Business systems. For this purpose, the **CLS Connect** flag must be activated.

NOTICE: After activation, this flag cannot be switched off.

If the system loses the connection to CLS, the failover period starts. If the connection is not reinstated after 30 days, the system gets in emergency mode, and it is considered as unlicensed.

NOTICE: When an OpenScape Business system with active CLS connect must be reprogrammed a backup file cannot be created. A reload must be performed with the same MAC ID and SIEL ID. The CLS connect cannot be activated without an active Base license. The existing license file from the CLS can be uploaded manually into the system via the WBM.

8.3.1.1 How to Activate CLS Connect

CLS connect allows you to make unlimited rehosts of your OpenScape Business systems.

Prerequisites

You are logged on to the WBM with the **Advanced** profile

You need Internet access to connect to the CLS

The following firewall settings are in place:

a) Port 7790 is released for outgoing IP traffic

Newer V3R3 software systems utilize port 7791 for online license activation.

b) IP 188.64.16.4 is released for outgoing IP traffic

NOTICE: To make the firewall rules more secure it is recommended to allow only outgoing communication.

The connection to CLS is possible; see How to check Central License Server (CLS) Connection

---

NOTICE: When you activate the CLS Connect, it is not possible to deactivate it.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click **Activate CLS Connect**.
3) Activate the **CLS Connect** by selecting the check box.
4) Click on **Activate**.

NOTICE: In the landing page notification area, the following message will be displayed if the online license control is activated:

`'License mode: "CLS Connect".'`

8.3.1.2 Switching from CLS connect

Moving away from the CLS connect to a Permanent or PAYGO license.

If you are currently using a 'CLS Connect' license scheme and wish to move to a permanent or PAYGO license, there are a few steps you need to follow to ensure a smooth transition:

Step by Step

1) Activate the CLS Connect Stop feature for the license file of the system. This can be done by raising a CLS support ticket.
2) Activate a new license file for the OSBiz to reset the secure bit. Once this is done, you can then enable PAYGO or Permanent local license for the system on CLS. You will then receive a new file which you can activate on the system.

NOTICE: If you have a networked OSBiz environment licensed in CLS Connect, slave nodes will also have the secure bit set. If you plan to use a slave node as a separate standalone system with a non-CLS Connect license at some point, please raise a support ticket for the required steps.

8.3.2 Activating Licenses (Standalone)

After purchasing a product or feature, you must first activate the licenses provided with the product or feature. After successful activation of the licenses, the licenses are assigned.

Licenses can be activated by one of the following two methods:

- **Online license activation** (via the license authorization code)

  Using the WBM, the customer or service technician transmits the license authorization code to the Central License Server (CLS) via the Internet. Together with the LAC, the Locking ID of the communication system is used for license activation. The CLS creates a license file from the data and sends this back to the system, which then activates the licenses purchased.

  To access the CLS, you will need an Internet connection. The IP address of the CLS is saved in the WBM under **License Management** > **Settings** and can be changed by an administrator with the **Expert** profile if required.

  NOTICE: By default, port 7790 is used for the online license activation. This port must be enabled in the firewall of the customer network.

  Newer V3R3 software systems utilize port 7791 for online license activation.

  NOTICE: Before the online licensing can be performed, the registration data must first be entered correctly.

- **Offline license activation** (using the license file)

  The customer or service technician logs in at the Central License Server (CLS) and enters the license authorization code there along with the Locking ID of the communication system. The CLS generates a license file from the

data entered. The customer or service technician downloads the license file and copies it into the WBM. The system then actives the purchased licenses.

The IP address of the CLS is saved in the WBM under **License Management** > **Settings** and can be changed by an administrator with the **Expert** profile if required.

If the communication system is to be expanded, further licenses can be purchased. On purchasing more licenses, an additional License Authorization Code (LAC) with which the newly procured licenses can be activated is supplied.

NOTICE: Additionally purchased licenses can also be activated remotely.

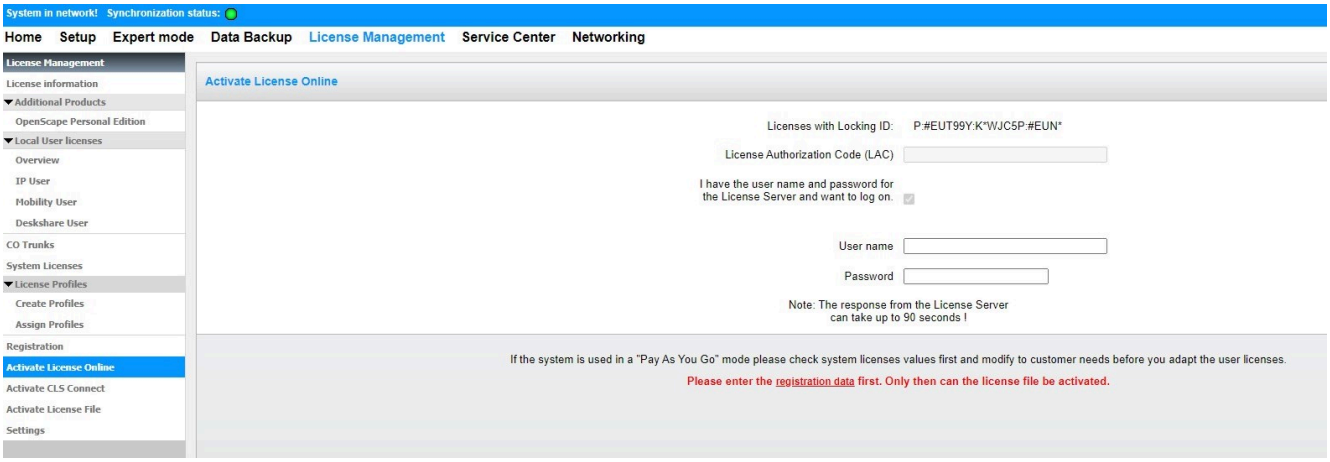
8.3.2.1 How to Activate Licenses Online (Standalone)

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

You know the License Authorization Code (LAC) needed to release the license.

In order to access the License server, the communication system must have access to the Internet.



Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **Registration**.
3) Enter your data and click **OK**.
4) In the navigation tree, click **Activate License Online**.
5) Enter the appropriate LAC in the **License Authorization Code (LAC)** field.
6) Select the check box **I have the user name and password for the License Server and want to log on**.
7) Enter the **User Name** and **Password** for logging into the License Server.

8) Click on **Activate**. The connection to the License Server is established, and the licenses are transferred to the communication system. Following the successful release, the connection is automatically reestablished.

8.3.2.2 How to Activate Licenses Offline (Standalone)

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The license file was generated earlier at the Central License Server and saved. You know the storage location of the license file.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click **Activate License File**.
3) Under **License File**, click **Browse** and select the storage location of the license file.
4) Click on **Activate**.

8.3.3 Assigning Licenses (Standalone)

Once the purchased licenses have been activated successfully, they must be assigned to the stations and lines. In a standalone system, system-wide features are enabled automatically upon activation.

Assigning User Licenses and User-oriented Licenses

Subscribers can be assigned user licenses and user-oriented licenses.

User licenses can be assigned to the following subscriber types:

Icon	User license	Description
	IP User	For the use of IP system telephones (HFA or SIP) and SIP telephones
	TDM User	For the use of UP0 system phones, ISDN phones, analog phones and DECT phones
	Mobility User	For the use of myPortal to go, Mobility Entry and DISA (One Number Service)
	Deskshare User	For the use of Desk Sharing by IP stations

The user licenses are permanently assigned to the numbers of the subscribers. If a subscriber is deleted or if another subscriber type is assigned to a call number, the associated user license is released.

There is a red asterisk next to some licenses. This red asterisk indicates that these licenses can also be covered by assigning another license.

With the flexible licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM,

DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

After a user license has been assigned to the subscriber, a user-oriented license can also be assigned to that subscriber.

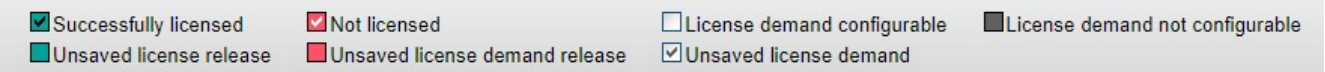
The following user-oriented licenses can be assigned to the stations:

Icon	User-oriented license	Description
	Voicemail	For the use of the voicemail box.
	Groupware user	For the use of the UC Suite features via myPortal for Outlook.
	UC User	For the use of the UC Suite features via myPortal for Desktop.
	Fax	For use of a fax box within the UC Suite. As a prerequisite, one UC User or Groupware User license is required.
	Conference	For use of the UC Suite conference features. As a prerequisite, one UC User or Groupware User license is required.
	myAttendant	For use of the UC Suite Attendant features.
	myAgent	For the use of Contact Center functions.
	Application Launcher	For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information.
	Unify Phone	For the use of the Unify Phone client in combination with OpenScape Business.
	TAPI	For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors.

You can have an overview of all user licenses and user-oriented licenses displayed (via **Local User Licenses** > **Overview)**.

This overview also shows the statuses of the licenses for each subscriber.

Possible license states:



Assigning System Licenses

System licenses include licenses for trunks and for system-wide features.

Licenses can be assigned to the following types of trunks:

- S_{2M}/T1 trunks: number of B channels
- ITSP trunks: number of simultaneous calls conducted via a single ITSP

In a standalone system, licenses for system-wide features will have already been unlocked by default during the license activation. Consequently, no further assignment is required.

License assignment procedure

Prerequisite: The license file is activated and the stations are configured.

- How to License Stations

  1) Assign a user license to a subscriber. This assignment triggers the generation of a license request for the subscriber while at the same time enabling the assignment of the user-oriented licenses.

  2) Assign the user-oriented licenses to a subscriber. These assignments cause further license requests to be generated for the subscriber. Please note that some licenses require other licenses (see Possible License Combinations).

  3) Check and unlock license requests.

  4) If there are not enough licenses to be unlocked, the invalid assignments will be displayed via the license statuses (in red). Correct the license assignments and then check and unlock the licenses again.

  NOTICE: To obtain a better overview, you can have the license assignments for all subscribers printed out as a preview (via **Local User Licenses** > **Overview** > **Print**). At the end of the printout, all invalid assignments are listed in a separate table.

- Assign trunk licenses

  The trunk licenses must be distributed to the required S_{2M}/T1 and ITSP trunks.

8.3.3.1 How to License Subscribers (Standalone)

Assign the available station licenses and user-oriented licenses to the subscribers. Once the licenses have been assigned successfully, the subscribers are licensed.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.

2) In the navigation tree, navigate to the desired type of subscriber under **Local User Licenses** > **...**. You will be shown a list of all subscribers of the selected subscriber type.

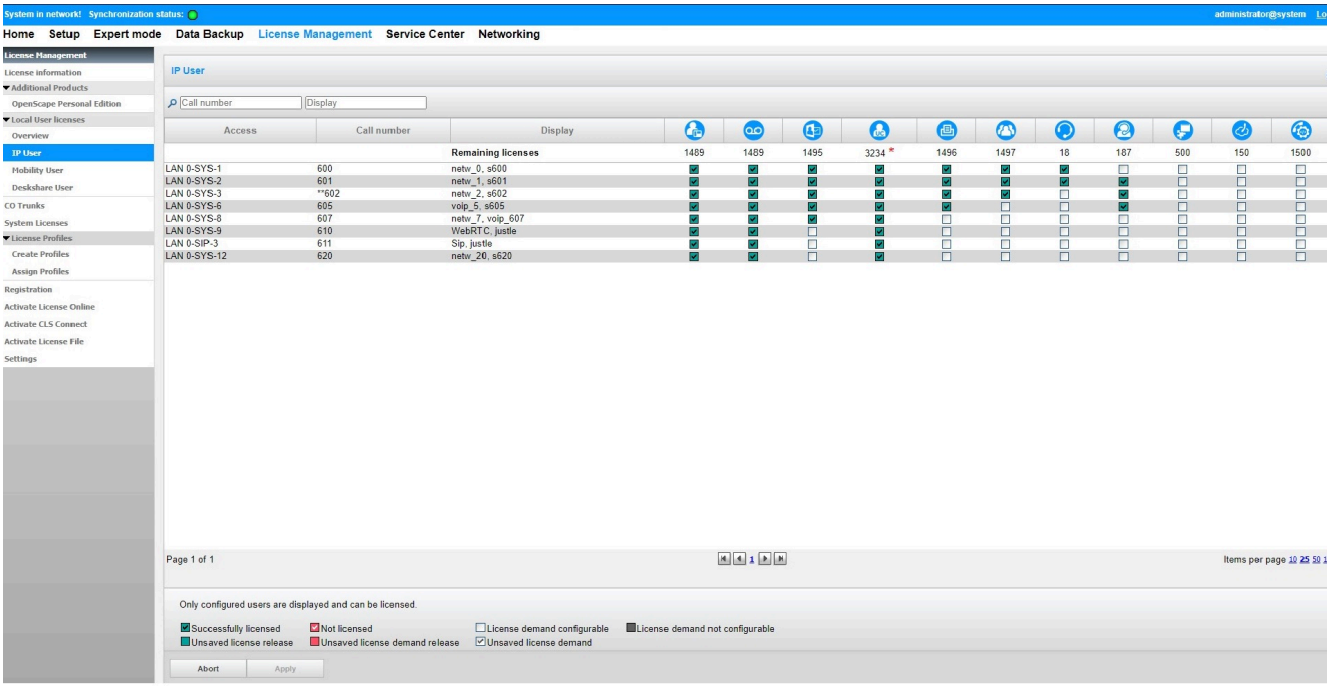
Under **Remaining licenses**, you will see how many licenses you can still assign to subscribers. For TDM, Mobility and Deskshare stations, the display includes all remaining IP User licenses as well, since these licenses can also

be used for the licensing of TDM, Mobility and Deskshare stations (flexible user licensing).

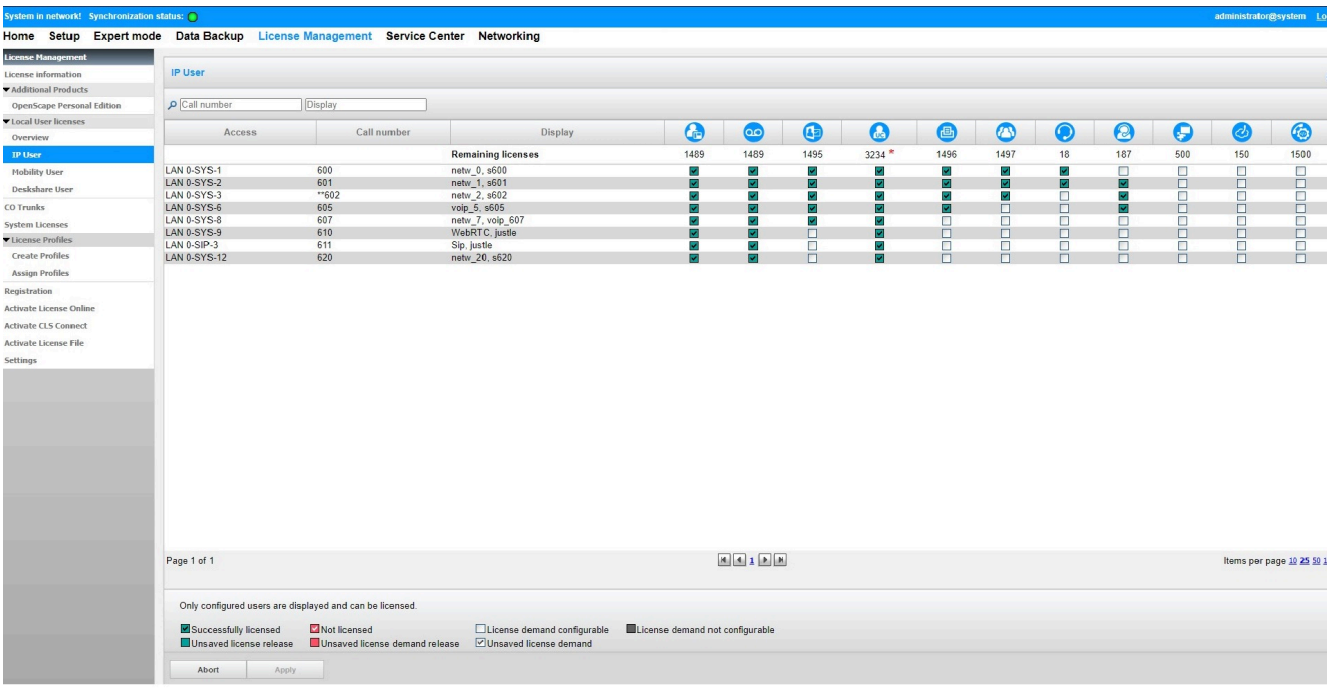
If the selected subscriber type is Mobility User, you will also see the total number of available Unify Phone licenses and their expiration date.

3) Activate the station license in the row of the desired subscriber by selecting the highlighted check box with a bright background (first column with check boxes). The check boxes in the other columns are enabled.

NOTICE: You can also have a selected station displayed by entering a search term in the **Station Number** or **Name** search fields and then pressing the Enter key or clicking the magnifying glass icon. All stations will be listed if you leave both search fields empty and then press the Return key or click on the magnifying glass icon.



4) Activate the user-oriented licenses in the row of the desired subscriber by selecting the appropriate check boxes.



NOTICE: User-oriented licenses can be assigned to a subscriber only if a station license was assigned to the subscriber earlier (step 3).

NOTICE: When assigning a VoiceMail license to an extension, a UC Suite user is created and all active call forwardings are reset.

NOTICE: In case of "Pay As You Go" voicemail license is checked/unchecked automatically whenever a voice user license is licensed/unlicensed but it is still possible to uncheck a voicemail license.

Groupware, UC User, Fax, myAttendant and myAgent license features are not configurable in UC Smart mode.

Groupware and UC User licenses are mutually exclusive in UC Suite mode.

5) Click **OK & Next**. A check is performed to determine whether there are enough licenses for your assignment.

If sufficient licenses are available, this completes the licensing of the subscriber.

NOTICE: In case of "Pay As You Go" a pop up window appears. Click on **OK** in order to confirm your choice.

6) If licenses are missing, the errors are indicated by displaying a check box shaded in red. Correct these errors and repeat step 5.

NOTICE: To remove a station license, you must acknowledge a warning message. After this, a new check box **Warnings enabled** appears. If you clear this check box, you can remove further station licenses without the warning.

8.3.3.2 How to License Trunks (Standalone)

Assign the purchased trunk licenses to SIP and S_{2M}/T1 trunks.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.

2) In the navigation tree, click **CO trunks**. The number of licenses available for SIP and S**2M**/T1 trunks is displayed in the $_{Trunks}$ area.

3) For SIP trunks: In the **SIP trunks** area, under **License demand for number of simultaneous Internet calls in this node**, enter the number of Internet calls that can be conducted simultaneously via an ITSP.

4) For S_{2M} trunks: In the **PRI (S2M/T1)** area, in the row of the desired S_{2M} slot, select the number of desired B-channels in the drop-down list of the **Demands** column.

5) For digital T1 trunks (U.S. only): In the **PRI (S2M/T1)** area, in the row of the desired T1 slot, select the number of desired B-channels in the drop-down list of the **Demands** column.

6) For analog T1 trunks (U.S. only): Activate the analog T1 line in the **PRI (S2M/T1)** area by selecting the entry **1** (**0** means the line is disabled) in the drop-down list of the **Demands** column in the row of the analog T1 line).

7) Click on **OK & Next**.

NOTICE: The number of licensed SIP trunks and S_{2M}/T1 trunks must not exceed the number of trunk licenses available.

8.4 Licensing Multiple Communication Systems (Internetwork)

The licensing of a multiple communication systems must be performed in a specific sequence. This sequence is shown below for a sample internetwork consisting of one OpenScape Business S (master) and two OpenScape Business X3 (slave) systems.

When multiple OpenScape Business (nodes) systems are combined into an internetwork, licensing occurs centrally via a network license file, which is activated on the master node. In addition, each slave node in the internetwork

needs its own networking system license. The node with the largest bandwidth should be the master node.

The nodes in the internetwork are configured as a master node and slave nodes via the Network Wizard of the WBM. The master node contains the central license agent (central CLA; central Customer License Agent). All slave nodes in the internetwork use this CLA for the licensing. To enable this, the IP address of the master node must be made known to the slave nodes using the WBM.

Only one network license file exists for the entire internetwork. This file is bound to the master node via the node's locking ID. If an OpenScape Business S (SoftSwitch) is the master node, the network license file is bound to the master node via either the Locking ID of the Linux server of the SoftSwitch or the Advanced Locking ID of the SoftSwitch if the SoftSwitch is used in a virtual environment. The network license file is stored in the central CLA and contains all the license information of the internetwork. It can be activated only at the master node via the WBM. Only the master node has access to the CLS; at all other nodes, the access is disabled.

No node-specific licensing should be performed in the internetwork. If separate network files exist for each node, you can combine them into a network license file at the CLS.

Behavior during Network Problems (Failover)

If the connection to the master node and thus to the central CLA fails, the message "Failover Period" appears on the displays of the system telephones. During this failover period (max. 30 days), all nodes and their features continue to operate normally. Once the network problems have been resolved and the connection to the central CLA is restored, all nodes revert to the regular license status.

If the network problems cannot be resolved within the failover period, the nodes switch to operating in emergency mode. The entire internetwork will then need to be relicensed.

Licensing Procedure in the Internetwork Based on the Above Example

OpenScape Business S (Master) and both OpenScape Business X3 (Slave) systems are already installed, configured and combined to form an internetwork.

1) **License Authorization Code (LAC)**

   On purchasing licenses, the customer receives a License Authorization Code (LAC). The information on the licenses purchased are stored in the database of the Central License Server (CLS).

2) **OpenScape Business S as master node**

   The customer or service technician logs into the WBM of the OpenScape Business S and installs the OpenScape Business S as the master node by using the Network Wizard.

   The system has already been installed and configured and is running in the Activation Period (period of 30 days during which the licensing has to be completed).

3) **Locking ID of the master node**

   The customer or service technician notes the Locking ID or the Advanced Locking ID of the OpenScape Business S.

   For a description, see How to Check the Locking ID of the Communication System

4) **OpenScape Business X3 as slave nodes**

   The customer or service technician first logs into the WBM of the first OpenScape Business X3 and installs the first OpenScape Business X3 as a slave node by using the Network Wizard. This process is then repeated at the WBM of the second OpenScape Business X3.

   The systems have been installed and configured and are running in the Activation Period.

5) **Locking IDs of OpenScape Business X3**

   The customer or service technician notes the Locking IDs of the two OpenScape Business X3 systems.

   For a description, see How to Check the Locking ID of the Communication System

6) **License Activation**

   The customer or service technician logs in at the CLS and generates a network license file together with the license authorization code and the locking IDs. He or she then loads this file into the master node using the WBM.

   For a description, see How to Activate Licenses Offline (Internetwork)

   The system then actives the purchased licenses.

7) **Assigning Licenses**

   The customer or service technician now distributes the licenses to the nodes. To do this, he or she logs into the WBM of each node and assigns the desired number of licenses to the node. Note that it is important that each node be assigned a networking system license; otherwise, it will not be integrated into the internetwork.

   For a description, see How to Assign System Licenses to a Node

8.4.1 License Activation (Internetwork)

After purchasing a product or feature, you must first activate the licenses provided with the product or feature. A license file is is used for license activation. After successful activation of the licenses, the licenses are assigned.

Licenses can be activated as follows:

- **Offline license activation** (using the license file)

  The customer or service technician logs in at the Central License Server (CLS) and enters the license authorization code there along with the Locking IDs of the communication systems. The CLS generates a license file from the data entered. The customer or service technician downloads the license file and copies it into the WBM of the master node.

  The master node is checked to see whether the Locking IDs stored in the license file match those of the systems. If the check is successful, the

licenses are activated, and the systems switch to the regular license status. If the check is not successful, the systems continue to run in the activation period until it expires and then only in emergency mode.

The IP address of the CLS is saved in the WBM under **License Management** > **Settings**.

License files can be combined as follows:

- **How to Combine License Files into a Network License File**

  If one or more nodes that have already been licensed are to be combined into an internetwork, the administrator must combine the individual license files via the CLS into a single license file and load it into the central CLA. The IP address of the master node with the central license agent must then be entered at all other nodes by using the WBM's network wizard.

8.4.1.1 How to Activate Licenses Offline (Internetwork)

This example describes the generation and activation of the shared network license file consisting of one OpenScape Business S as a master node (Node 1) and two further OpenScape Business X3 systems (Node 2 and Node 3).

Prerequisites

Access to the CLS exists.

All nodes are installed and networked with one another; see Networking OpenScape Business X and OpenScape Business S (Multi-Gateway) .

Step by Step

1) Log into the CLS with your user name and password.
2) Under **Licenses**, select the item **Generate and download license key**.
3) Enter the License Authorization Code (LAC) under **LAC** and click **Search**.
4) Open the OpenScape Business S product and select the features to be assigned to Node 1.
5) Click on **Generate License Key**.
6) Enter the MAC address or the Advanced Locking ID of OpenScape Business S (Node 1) under **MAC Address** and then enter the MAC address or the Advanced Locking ID of OpenScape Business S of Node 1 (master node) again under **MAC Address of the Network CLA**.

   NOTICE: The MAC address of OpenScape Business S is the MAC address of the network card of the OpenScape Business S Linux server that was used when installing the Linux operating system. The Advanced Locking ID of OpenScape Business S is used instead of the MAC address when OpenScape Business S is operated in a virtual environment.

7) Enter the desired number for the features and click **Next**.
8) Verify the customer data and click **Next**.
9) Read through the legal notification and then click **Yes, I agree to the terms of use!**.
10) Click on **Execute** to generate the license key.

11) For Node 2, under **Licenses**, select the item **Generate and download license key**.
12) Enter the License Authorization Code (LAC) again under **LAC** and click **Search**.
13) Open the OpenScape Business X3 product and select the features to be assigned to Node 2.
14) Click on **Generate License Key**.
15) Enter the MAC address of Node 2 under **MAC Address** and then enter the MAC address of Node 1 (master node) under **MAC Address of the Network CLA**.
16) Enter the desired number for the features and click **Next**.
17) Click on **Next**.
18) Confirm the legal notification by selecting the check box **Yes, I agree to the terms of use!**.
19) Click on **Execute** to generate the license key.
20) Repeat steps 11 through 19 for Node 3.
21) Click on **License Key** and then on **Download** to download the network license file.
22) Save the network license file.
23) Log into the WBM of the master node by calling up the address `https://<IP address of the master node>` in your web browser and then entering your user name and password.
24) Click on **License Management** in the navigation bar.
25) In the navigation tree, click **Activate License File**.
26) Under **License File**, click **Browse** and select the storage location of the network license file.
27) Click on **Activate**.

8.4.1.2 How to Combine License Files into a Network License File

If several nodes that were previously not networked are subsequently integrated into an internetwork, the license files of the individual nodes must be combined into a common network license file with the help of the CLS.

Prerequisites

Access to the CLS exists, and you have the access rights for the license packages of the individual nodes.

All nodes are installed and networked with one another; see Networking OpenScape Business X and OpenScape Business S (Multi-Gateway) .

Step by Step

1) Log into the CLS with your user name and password.
2) Under **Network Licensing**, select the item **Add/Remove System**.
3) Select the MAC address of the node that is to be integrated in the internetwork.
4) Click on the **Rehost**.
5) Enter the MAC address of the node under **MAC Address**.

6) Enter the MAC address of the master node under **MAC Address of the Network CLA**. As a rule, OpenScape Business S is the master node.

NOTICE: The MAC address of OpenScape Business S is the MAC address of the network card of the OpenScape Business S Linux server that was used when installing the Linux operating system.

---

7) Click on **Next**.
8) Verify the customer data and click **Next**.
9) Read through the legal notification and then click **Yes, I agree to the terms of use!**.
10) Click on **Execute** to generate the license key.
11) Repeat steps 2 through 10 for further nodes.
12) Click on **License Key** and then on **Download** to download the network license file.
13) Save the network license file.
14) Log into the WBM of the master node by calling up the address `https://<IP address of the master node>` in your web browser and then entering your user name and password.
15) Click on **License Management** in the navigation bar.
16) In the navigation tree, click **Activate License File**.
17) Under **License File**, click **Browse** and select the storage location of the network license file.
18) Click on **Activate**.

8.4.2 Assigning Licenses (Internetwork)

Once the purchased licenses have been activated successfully, they must be assigned to the stations and lines. License assignment must be performed separately on each node.

Assigning User Licenses and User-oriented Licenses

Subscribers can be assigned user licenses and user-oriented licenses.

User licenses can be assigned to the following subscriber types:

Icon	User license	Description
	IP stations	For the use of IP system telephones (HFA or SIP) and SIP telephones
	TDM stations	For the use of UP0 system phones, ISDN phones, analog phones and DECT phones
	Mobile stations	For the use of myPortal to go, Mobility Entry and DISA (One Number Service)
	DeskSharing stations	For the use of Desk Sharing by IP stations

Icon	User license	Description
	Fallback user	For basic telephony use in case of an event of failure.

The user licenses are permanently assigned to the numbers of the subscribers. If a subscriber is deleted or if another subscriber type is assigned to a call number, the associated user license is released.

With the flexible licensing, TDM, Mobility and Deskshare users can also be licensed with IP user licenses. If all the acquired TDM, DeskShare and Mobility user licenses have already been assigned to subscribers, and further TDM, DeskShare and Mobility users are required, then any remaining IP User licenses can be used to meet this demand.

After a user license has been assigned to the subscriber, a user-oriented license can also be assigned to that subscriber.

The following user-oriented licenses can be assigned to the stations:

Icon	User-oriented license	Description
	Voicemail	For the use of the voicemail box.
	Groupware user	For the use of the UC Suite features via myPortal for Outlook.
	UC Suite	For the use of the UC Suite features via myPortal for Desktop.
	Fax	For use of a fax box within the UC Suite. As a prerequisite, one UC User or Groupware User license is required.
	Conference	For use of the UC Suite conference features. As a prerequisite, one UC User or Groupware User license is required.
	myAttendant	For use of the UC Suite Attendant features.
	myAgent	For the use of Contact Center functions.
	Application Launcher	For call-related control of applications on a client PC during incoming and outgoing calls, e.g., launching an application or displaying caller information.
	Unify Phone	For the use of the Unify Phone client in combination with OpenScape Business.
	TAPI 120/170	For the use of TAPI compliant applications and for PC-supported telephony with the customer's own applications from various software vendors.

You can have an overview of all user licenses and user-oriented licenses displayed (via **Local User Licenses** > **Overview)**.

This overview also shows the statuses of the licenses for each subscriber.

Possible license states:



Assigning System Licenses

System licenses include licenses for trunks and for system-wide features.

Licenses can be assigned to the following types of trunks:

- S_{2M}/T1 trunks: number of B channels
- ITSP trunks: number of simultaneous calls conducted via a single ITSP

System-wide licenses are assigned to every system (node) in the network. This configuration must be performed in direct succession (i.e., one after the other) at each node. The total number of system-wide licenses stored in the network license file on the master node is reduced by the number configured at the node.

License assignment procedure

Prerequisite: The license file is activated and the stations are configured.

- How to License Stations

  1) Assign a user license to a subscriber. This assignment triggers the generation of a license request for the subscriber while at the same time enabling the assignment of the user-oriented licenses.

  2) Assign the user-oriented licenses to a subscriber. These assignments cause further license requests to be generated for the subscriber. Please note that some licenses require other licenses (see Possible License Combinations).

  3) Check and unlock license requests.

  4) If there are not enough licenses to be unlocked, the invalid assignments will be displayed via the license statuses (in red). Correct the license assignments and then check and unlock the licenses again.

  NOTICE: To obtain a better overview, you can have the license assignments for all subscribers printed out as a preview (via **Local User Licenses** > **Overview** > **Print**). At the end of the printout, all invalid assignments are listed in a separate table.

- Assign trunk licenses

  The trunk licenses must be distributed to the required S_{2M}/T1 and ITSP trunks.

8.4.2.1 How to License Subscribers (Internetwork)

Assign the available station licenses and user-oriented licenses to the subscribers. Once the licenses have been assigned successfully, the subscribers are licensed.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

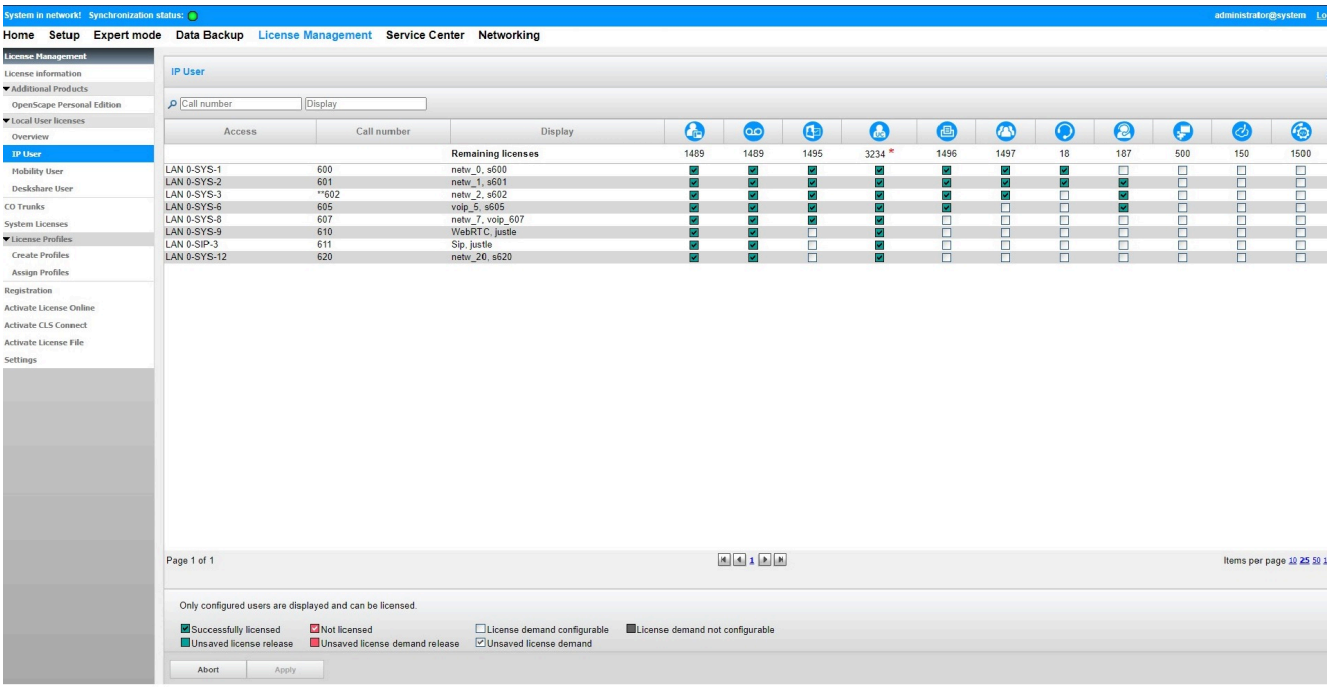
Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, navigate to the desired type of subscriber under **Local User Licenses** > **...**. You will be shown a list of all subscribers of the selected subscriber type.

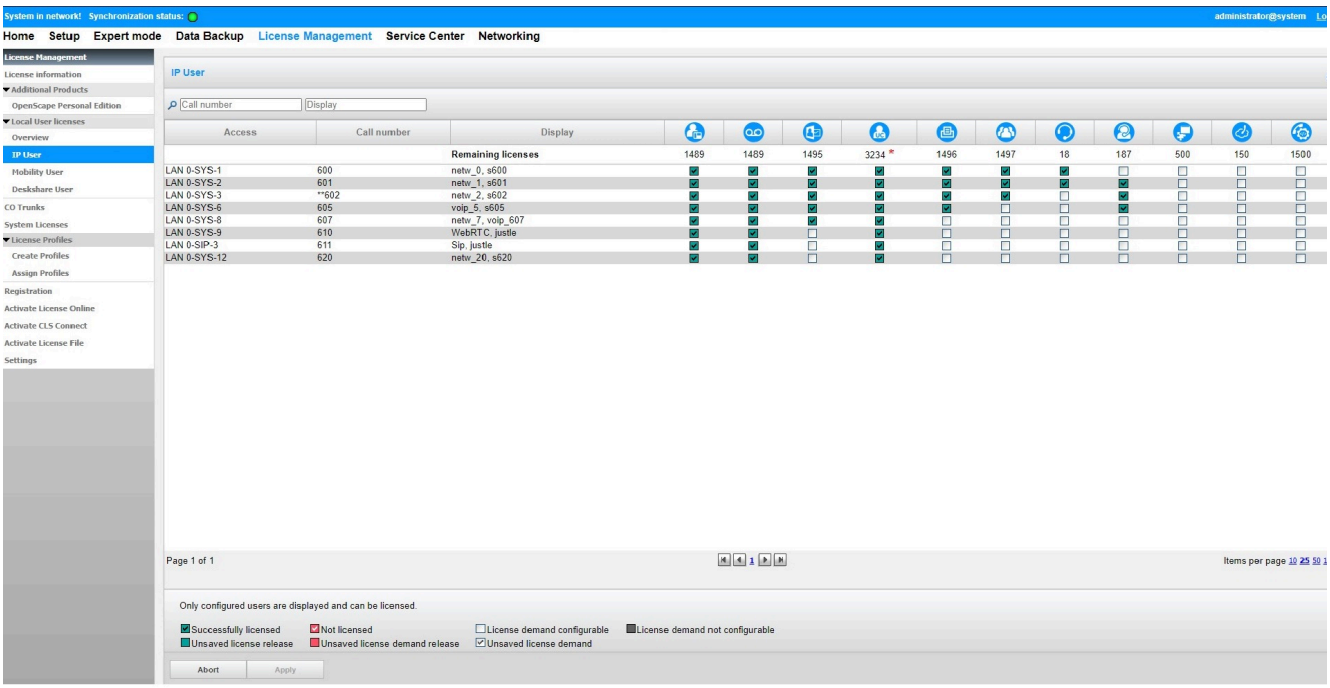
   Under **Remaining licenses**, you will see how many licenses you can still assign to subscribers. For TDM, Mobility and Deskshare stations, the display includes all remaining IP User licenses as well, since these licenses can also be used for the licensing of TDM, Mobility and Deskshare stations (flexible user licensing).

   If the selected subscriber type is Mobility User, you will also see the total number of available Unify Phone licenses and their expiration date.
3) Activate the station license in the row of the desired subscriber by selecting the highlighted check box with a bright background (first column with check boxes). The check boxes in the other columns are enabled.

NOTICE: You can also have a selected station displayed by entering a search term in the **Station Number** or **Name** search fields and then pressing the Enter key or clicking the magnifying glass icon. All stations will be listed if you leave both search fields empty and then press the Return key or click on the magnifying glass icon.



4) Activate the user-oriented licenses in the row of the desired subscriber by selecting the appropriate check boxes.



NOTICE: User-oriented licenses can be assigned to a subscriber only if a station license was assigned to the subscriber earlier (step 3).

NOTICE: "Pay As You Go" is not available in case of network license file.

In case of a network of OpenScape Business systems, any of the systems can utilize Pay As You Go via local Central License Agent (CLA).

5) Click **OK & Next**. A check is performed to determine whether there are enough licenses for your assignment.

   If sufficient licenses are available, this completes the licensing of the subscriber.

6) If licenses are missing, the errors are indicated by displaying a check box shaded in red. Correct these errors and repeat step 5.

NOTICE: To remove a station license, you must acknowledge a warning message. After this, a new check box **Warnings enabled** appears. If you clear this check box, you can remove further station licenses without the warning.

8.4.2.2 How to License Trunks (Internetwork)

Assign the purchased trunk licenses to SIP and S_{2M}/T1 trunks.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click **CO trunks**. The number of licenses available for SIP and S_{2M}/T1 trunks is displayed in the **Trunks** area.
3) For SIP trunks: In the **SIP trunks** area, under **License demand for number of simultaneous Internet calls in this node**, enter the number of Internet calls that can be conducted simultaneously via an ITSP.
4) For S_{2M} trunks: In the **S2M** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
5) For T1 trunks (only for the U.S.): In the **T1** area, in the row of the desired slot, select the number of desired B-channels in the drop-down list of the **Demands** column.
6) Click on **OK & Next**.

NOTICE: The number of licensed SIP trunks and S_{2M}/T1 trunks must not exceed the number of trunk licenses available.

8.4.2.3 How to Assign System Licenses to a Node

Prerequisites

You are logged on to the WBM of the desired node.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click on **System Licenses** in the navigation tree. All available system licenses are displayed.
3) Locate the desired system licenses in the **used licenses** column and select the number of system licenses to be assigned to the node.

   The **available for distribution** column indicates how many licenses are available for the entire internetwork.

NOTICE: Make sure that the node is assigned the "Networking" system license, otherwise the node will fail to be integrated into the internetwork.

---

4) Click on **Save**.

8.4.2.4 How to Assign the "Networking" System License to a Node

Prerequisites

You are logged on to the WBM of the desired node.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click on **System Licenses** in the navigation tree. All available system licenses are displayed.
3) For the **Networking** system license, select **1** from the drop-down list in the **used licenses** column.

   The **available for distribution** column indicates how many licenses are available for the entire internetwork.
4) Click on **Save**.

8.5 License information

Information on the available and assigned licenses, products and features is displayed with the WBM. The license information on all nodes available in the internetwork can be retrieved.

The following information can be displayed:

- **MAC Address**: MAC address of the hardware platform or the Linux Server SoftSwitch to which the licenses are bound.

  NOTICE: If the communication system is in the activation period, a wrong MAC address may possibly be shown here. The correct MAC address can be checked via the **Service Center** under **Inventory** (Inventory).
- **Advanced Locking ID**: Advanced Locking ID of the softswitches in a virtual environment, to which the licenses are bound.
- **Locking ID**: Locking ID of the Application Server to which the licenses are bound.
- **Node**: Name of the communication system to which the license is bound.
- **Product Name**: Name of the product for which the license is assigned.
- **Feature**: Feature for which the license has been assigned.
- **Used licenses**: Shows the number of used and available licenses.
- **Available for distribution**: Shows the licenses still available in the internetwork.
- **Status**: Status of the license.

The OpenScape Personal Edition product is licensed by its own license file. The license information for this is displayed under **Additional Products**.

8.5.1 License Information without a Network (Standalone)

All licenses assigned to the communication system and the relevant licensing information can be displayed.

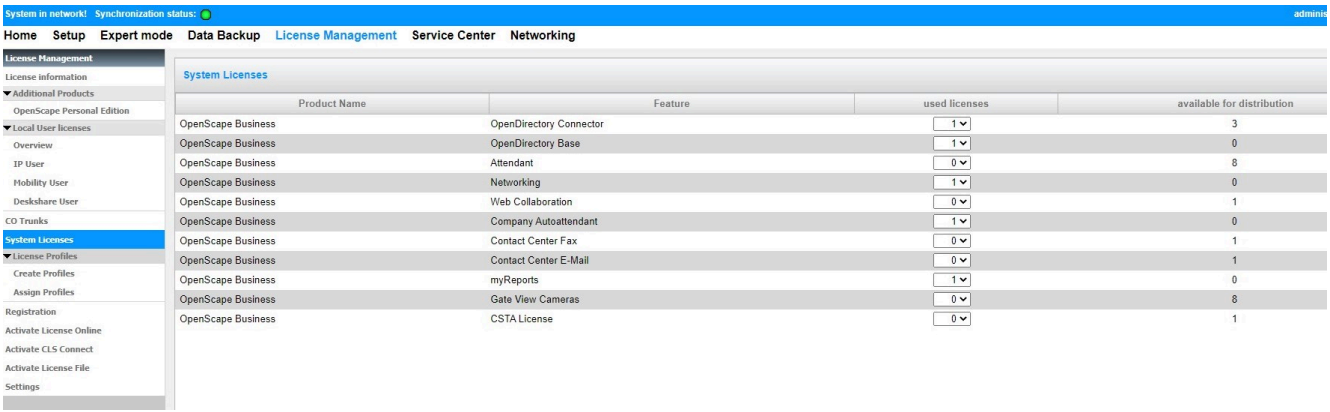
8.5.1.1 How to Display License Information

Prerequisites

You are logged in at the WBM.

Step by Step

Click on **License Management** in the navigation bar. The license information for your communication system will be displayed.



NOTICE: In case of "Pay As You Go" used licenses are configurable except for Contact Center Fax, Contact Center E-mail and myReports in UC Smart mode.

8.5.2 License Information in an Internetwork

In an internetwork, all existing licenses and the relevant license information can be displayed. This information is read from the network license file.

All licenses of an internetwork (with the exception of the base licenses) are "floating" licenses and are managed in a license pool. If a license is no longer required by a node (communication system), it is released and can thus be used another node.

All the licenses of the internetwork as well as any shared (floating) licenses or licenses that are bound to a specific node can be displayed in an internetwork.

In addition, station licenses and user-oriented licenses can be sorted by node and displayed in a list.

8.5.2.1 How to Display all Licenses in the Internetwork

Prerequisites

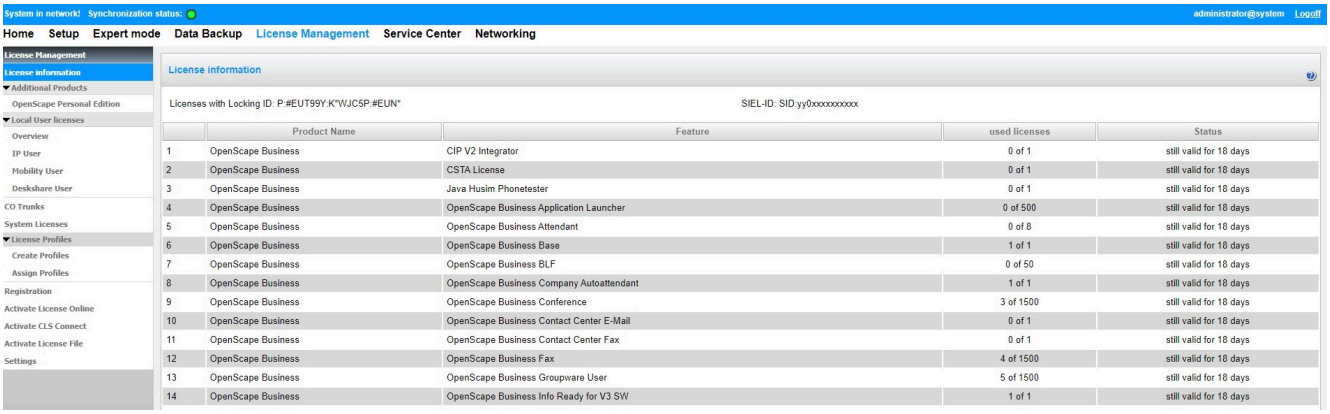
The communication system is located in an internetwork.

You are logged in at the WBM.

Step by Step

1) Click on **License Management** in the navigation bar.

2) In the navigation tree, click on **License Information**. All licenses in the internetwork are displayed.



8.5.2.2 How to Display the Licenses Bound to a Node

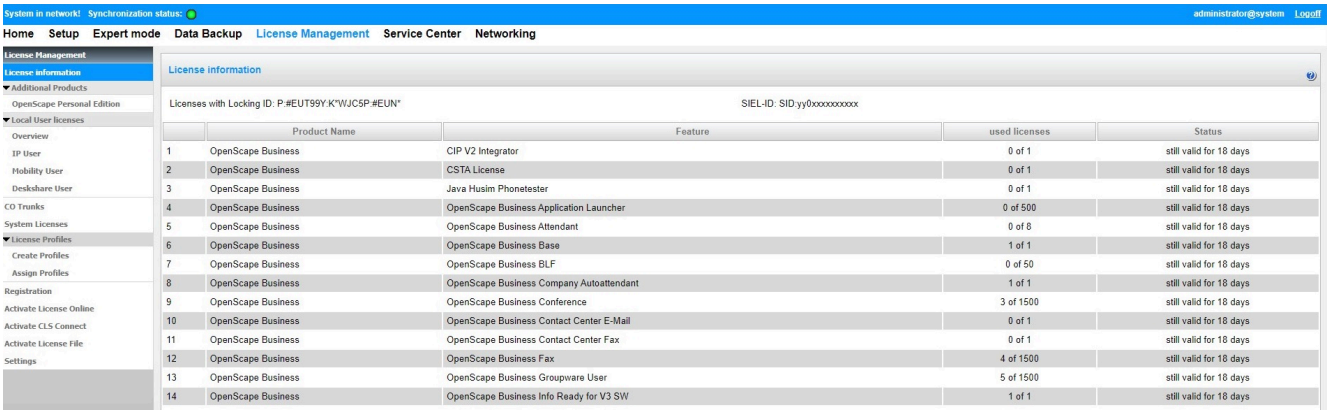
Prerequisites

The communication system is located in an internetwork.

You are logged in at the WBM.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **License Information**.
3) Click in the navigation tree on the system name or the locking ID of the desired node. The licenses specifically bound to this node will be displayed, e.g., the base license.



8.5.2.3 How to Display all Shared Licenses in an Internetwork

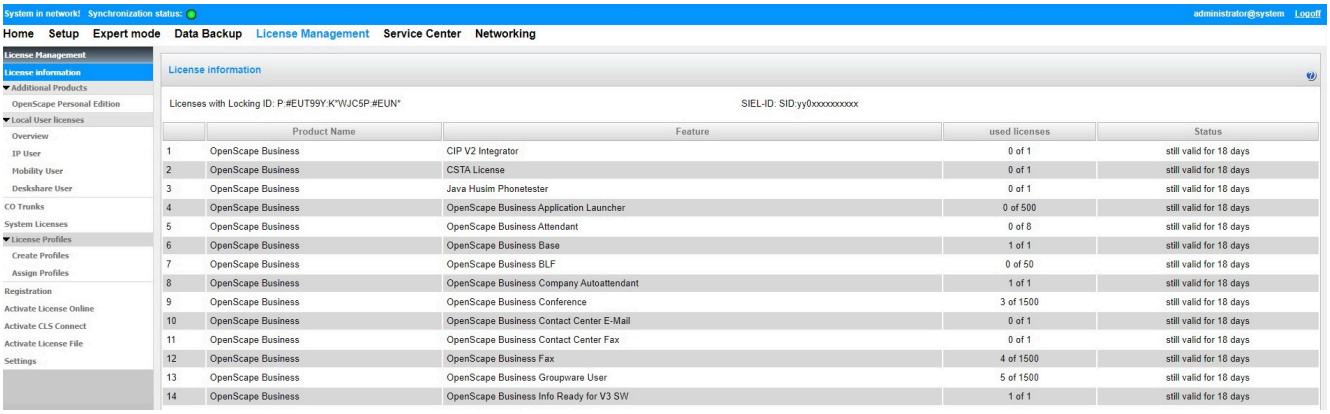
Prerequisites

The communication system is located in an internetwork.

You are logged in at the WBM.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **License Information**.
3) In the navigation tree, click **Floating**. All shared licenses in the internetwork are displayed.



	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 How to Display a Node-Dependent View of Station Licenses and User-Oriented Licenses

Prerequisites

The communication system is located in an internetwork.

You are logged in at the WBM.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click on **Network-wide License Overview** in the navigation tree. All station licenses and user-oriented licenses in the internetwork can be sorted by node.

8.6 Assigning License Profiles

License profiles contain predefined license assignments and can be assigned to one or more stations. License profiles are useful if more than one subscriber is to receive same license.

You can use predefined license profiles or create new license profiles.

A license profile only applies to one station type and can only be assigned to stations of this type. Several license profiles can be created and named appropriately for a station type.

License profiles can be created for the following types of stations:

- IP stations (IP system phones, SIP phones)
- TDM stations (UP0 phones, ISDN phones, analog phones, DECT phones)
- DeskSharing stations
- Mobile stations

Within a license profile, you can assign assign user-oriented licenses to the station type as needed.

If the license assignment for a station within a license profile is changed, the assignment of the station to the license profile is automatically revoked.

8.6.1 How to Add a License Profile

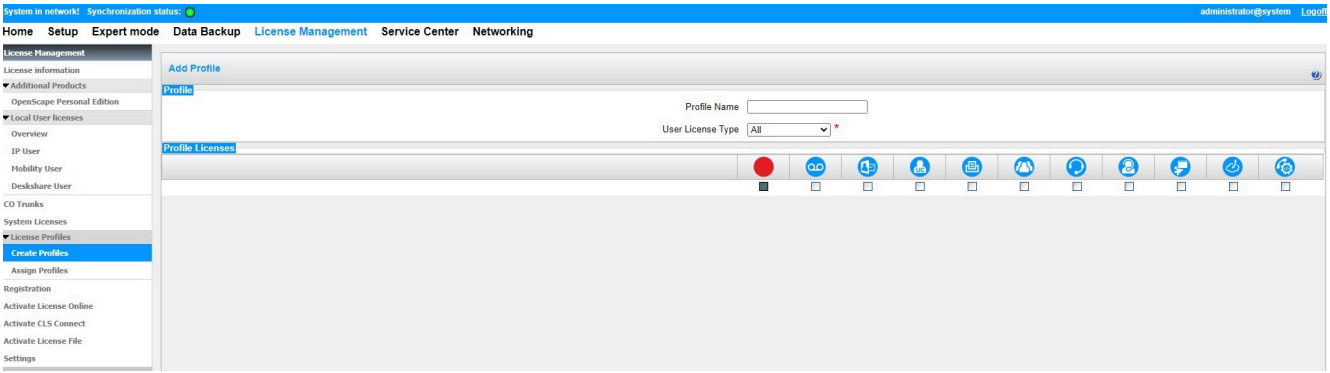
Create a new license profile.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click in the navigation tree on **License Profiles** > **Create Profiles**. All existing license profiles are displayed.
3) Click on **Add**.



4) In the **Profile Name** field, enter a name of your choice for the new profile.
5) Select the subscriber type to which the profile is to be applied from the **User License Type** drop-down list.
6) Select the user-oriented licenses by activating the appropriate check boxes.
7) Click on **OK & Next**. A check is performed to see whether the licenses are assigned correctly.

   If all licenses are assigned correctly, the licensing of subscribers is considered to be complete.
8) If any of the licenses are assigned incorrectly, their check boxes will be shaded in red. Correct these errors and repeat step 7.

8.6.2 How to Edit a License Profile

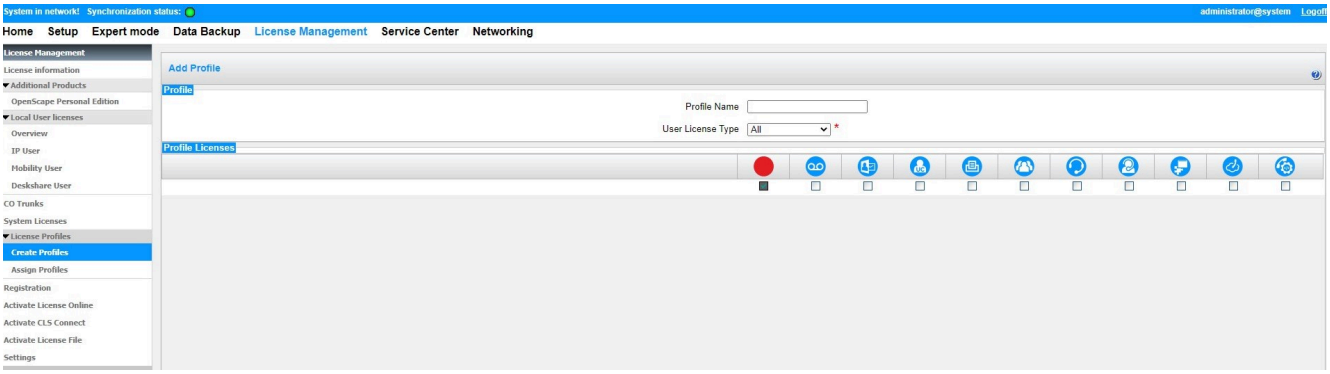
Edit an existing license profile.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click in the navigation tree on **License Profiles** > **Create Profiles**. All existing license profiles are displayed.



3) Activate the radio button in front of the desired license profile and click **Edit**.
4) Edit the license profile as desired.
5) Click on **OK & Next**. A check is performed to see whether the licenses are assigned correctly.

   If all licenses are assigned correctly, license profile editing is complete.
6) If any of the licenses are assigned incorrectly, their check boxes will be shaded in red. Correct these errors and repeat step 5.

8.6.3 How to Assign a License Profile to Stations

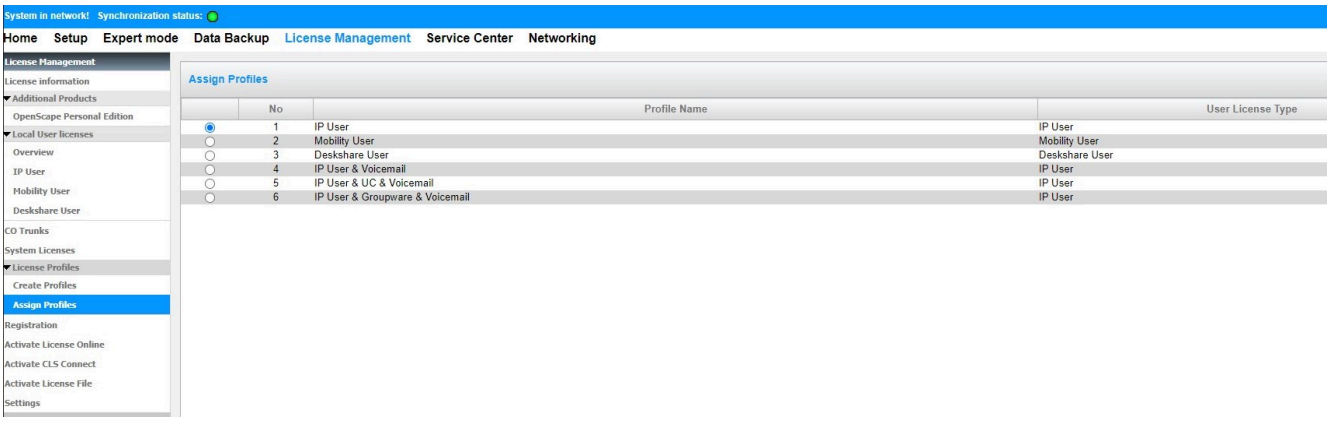
Assign a license profile to the available stations.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click in the navigation tree on **License Profiles** > **Assign Profiles**. All existing license profiles are displayed.



3) Activate the radio button in front of the desired license profile and click **OK & Next**.

4) Under **Selection** on the left, select all stations to which the license profile is to be assigned.
5) Click on **Add**. The selected stations appear in the **Members** window on the right.
6) Click on **OK & Next**. The licenses selected in the license profile are assigned to the stations.

NOTICE: In case of "Pay As You Go" a pop up window appears. Click on **OK** in order to confirm your choice.

NOTICE: Stations can also be removed from a license profile or added to it later.

8.6.4 How to Delete a License Profile

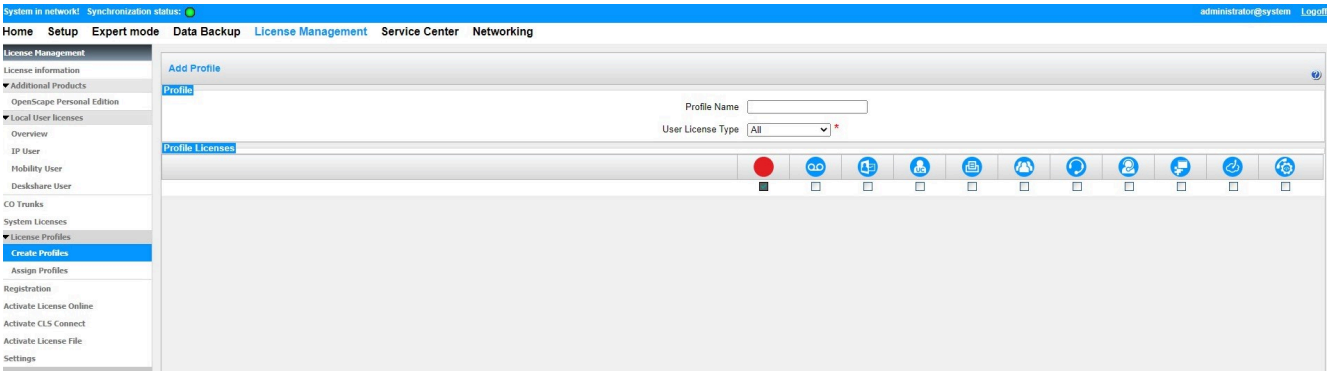
Delete an existing license profile.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **License Management** in the navigation bar.
2) Click in the navigation tree on **License Profiles** > **Create Profiles**. All existing license profiles are displayed.



3) Activate the radio button in front of the desired license profile and click **Delete**.
4) Confirm the message with **OK**. The license profile is deleted.

8.7 Rehosting after Replacement of Hardware

Licenses must be updated whenever the mainboard of the hardware platform or the network card of the Linux server is replaced at the communication system. Rehosting requires the MAC address of the old hardware, the MAC address of the new hardware and the login credentials for the central license server (CLS).

After replacing the hardware, the configuration data must be restored using the latest backup set (see Restore).

Since the licenses are bound to the MAC address of the hardware, the MAC address changes on replacing the hardware, and the licenses are thus are no longer valid. After a hardware replacement, the communication system reverts to the activation period. After the old and new MAC addresses have been entered at the CLS, the new license file can be generated. This is loaded into the communication system through via an offline update, and all existing licenses are then activated automatically.

For the softswitch, the MAC address of the network card of the Linux server, which was selected on installing the Linux operating system (visible via YaST), is used. The MAC address can also be read by using the WBM.

NOTICE: Every rehost is logged on the CLS. A license can be used for a rehost up to three times.

NOTICE: The IP address of the CLS can be checked via the WBM under **License Management** > **Settings** and changed if required.

8.7.1 How to Perform a Rehost after Replacing Hardware

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The hardware has been replaced, and you have performed a rehost at the CLS.

The configuration data has been restored using the latest backup set.

You know the License Authorization Code (LAC) needed to release the license.

In order to access the License server, the communication system must have access to the Internet.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click **Activate License Online**.
3) Enter the appropriate LAC in the **License Authorization Code (LAC)** field.
4) Leave the check boxes for accessing the License server via a user name and password disabled. Access to the Licensing Server occurs automatically. (The input of a user name and password is only required for sales partners.)
5) Click on **Activate**. The connection to the license server is established and the licenses are released. Following the successful update, the connection is reestablished automatically.
6) Restart the communication system.

Next steps

Save your configuration data in a new backup set (see Immediate Backup).

8.8 License Server (Central License Server, CLS)

The Central License Server (CLS) generates and manages the license files.

A license file is generated when the customer sends the License Authorization Code (LAC) to the CLS via the WBM. The transmission of the license file to the communication system occurs automatically via the Internet. If an automatic transmission is not possible, the license file can also be loaded manually into the communication system.

8.8.1 How to Check or Change the IP Address of the License Server

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

If the IP address of the Central License Server has changed, you will need to know the current IP address.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **Settings**. The IP address of the Central License Server (CLS) appears in the **IP address of the Central License Server** field. The currently valid IP address is `188.64.16.4`.
3) If you need to change the IP address of the Central License Server, enter the new IP address of the Central License Server in the corresponding **IP address of the Central License Server** field in the format `123.124.125.126`.
4) Click on **Activate**.

8.8.2 How to check Central License Server (CLS) Connection

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **Settings**.
3) In the **Central License Server** area, click on **Test CLS Connection**.

If there is an active internet connection, the **Successfully Connected to CLS!** message appears.

If there is no internet connection, the **No connection to CLS!** message appears.

8.9 Customer License Agent (CLA)

The Customer License Agent (CLA) is part of the OpenScape Business communication software and runs automatically in the background. It manages the license file and the licenses contained therein. The CLA checks the license requirements, and if sufficient licenses are available, it activates the licenses. There is only one CLA (local CLA) for each communication system. If several

communication systems (nodes) are present in one internetwork, only one CLA (central CLA) should be used on the master node.

The following configurations are possible:

- **How to Configure the Connection to the Local License Agent**

  When a node is removed from the internetwork, the connection to the central CLA will be cleared. The local CLA installed on the node is used automatically instead. If this automatic mechanism fails, the connection to the local CLA can also be made manually.
- **How to Change the Connection to the Central License Agent**

  Every node in the internetwork requires the connection to the Central CLA on the master node. This connection is automatically established on running the WBM wizard **Network**. If the IP address of the master node changes, the connection to the central CLA must be reconfigured at all slave nodes.

8.9.1 How to Configure the Connection to the Local License Agent

Prerequisites

You are logged on to the WBM of the desired node.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **Settings**.
3) Enable the **Customer License Agent (CLA) Local Host** radio button.
4) Click on **Activate**.

8.9.2 How to Change the Connection to the Central License Agent

Prerequisites

The communication system is located in an internetwork.

You are logged on to the WBM of the desired node.

Step by Step

1) Click on **License Management** in the navigation bar.
2) In the navigation tree, click on **Settings**.
3) Enable the **Central License Agent** radio button and enter the IP address of the master node (node 1) under **IP address of Central License Agent** in the format `123.124.125.126`.
4) Click on **Activate**.

8.10 Locking ID and Advanced ID Locking

Each communication system is assigned a Locking ID or an Advanced Locking ID. To ensure a unique assignment of licenses, the licenses are tied to these Locking IDs.

Locking ID

With hardware platforms, the Locking ID is the MAC address of the communication system.

With softswitches, the Locking ID is the MAC address of the network card of the Linux server. If the Linux server has multiple network cards, the network card that was used at initial startup of the Linux server must be selected.

If the communication system is in the activation period, a wrong MAC address may possibly be shown under the license information. The correct MAC address can be checked via the **Service Center** under **Inventory**.

Advanced Locking ID

If a softswitch runs in a virtual environment, the Advanced Locking ID (ALI) is used instead of the Locking ID. The Advanced Locking ID is generated at the CLS using the ALI Calculator.

The following system and network parameters must be configured, since they are used to generate the 24-digit Advanced Locking ID.

- IP address of the default gateway (Linux server)
- Host name of the Linux server
- IP address of the Linux server
- IP address of the DNS server (configured in the Linux server)
- Time zone (Linux server)

If one or more of these system and network parameters are not set, then the Advanced Locking ID cannot be generated.

The Advanced Locking ID is displayed in the WBM. In some cases, it is possible that the ALI which was generated at the CLS for the license file may differ from the ALI which is displayed during the activation period in the WBM. The license file containing the deviant ALI is accepted by the system anyway.

If any of the system and network parameters listed above changes, the softswitch reverts to the unlicensed state, and a new Advanced Locking ID is generated. In order to be able to use the purchased license again, a rehost from the old to the new Advanced Locking ID must be conducted at the Central License Server (CLS).

If the system detects a change in ALI, a message is displayed on the WBM home page in Licensing area to inform the user that ALI has been changed. The user has to click on Confirm, to verify for being informed about the change. Then the message is removed from the WBM home page, until a new instance of ALI change is detected. If the user does not click on Confirm, the message is permantly displayed on the home page.

IMPORTANT: If any change is made in the Locking ID parameters (IP address, Gateway address, DNS address, Hostname for S systems, MAC address for X systems), the sytem license becomes invalid. You should contact an authorized partner at the Cental License Server to generate a new lisence file and the new lisence file must be installed in the sytem.

IMPORTANT: If a user presses the confirm button, no email will be sent afterwards. An email will only be sent if the user hasn’t

confirmed the changes via Home page. Email mechanism is triggered every day with an 24h interval, starting from the last system restart.

8.10.1 How to Check the Locking ID of the Communication System

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) In the navigation tree, click **Inventory**. An overview of the components that make up the communication system is shown.
3) Click on **OK & Next**. Information on the hardware and software appears. The locking ID of the communication system can be found under **MAC ID for license**.

8.10.2 How to Check the Locking ID of the Softswitch

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) In the navigation tree, click **Inventory**. Information on the software of the softswitches, the available and used hard disk storage and on the application status will be displayed. The locking ID of the softswitch can be found under **MAC ID for license**.

8.10.3 How to Check the Advanced Locking ID of Softswitches

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

Click on **License Management** in the navigation bar. All existing licenses are displayed. If the softswitch is being operated in a virtualized environment, the advanced locking ID of the softswitch can be found under **Locking ID**.

8.11 How to migrate from V2 mainboard to V3 mainboard (standalone system)

Prerequisites

- Update to the latest system version.

- Unplug the IVM cards, clean the card slots and remove the IVM configuration from system.
- Make sure that the ports at range 511-532 are not configured. These ports will be reserved by SmartVM on V3 mainboard. This is needed only for systems operating in UC Smart mode.

  To address issues with the UC Fax functionality during migration to the V3 mainboard system, it is recommended to configure the system's operation mode prior to migration. If the system is operating in UC Smart mode, the administrator should delete the configuration from ports 511-532 before migration takes place. If the system is operating in UC Suite mode, the additional SmartVM ports will not be created and the fax configuration will not be affected. For instance, if the backup set is coming from a UC Suite system, the V3 mainboard system operation mode should be switched to UC Suite mode before migrating the backup set.

  NOTICE: When you upgrade an OpenScape Business PAYGO system, upgrade the Open Scape Business system to V3 software first and then use on the CLS **re-generate license key** function to receive a valid license file for V3 which has then the "OpenScape Business Info Ready for V3 SW F31505-K158-D129" license. After that, the re-generated license file needs to be activated manually within the OpenScape Business System WBM, under **License management**.

NOTICE: When you upgrade an OpenScape Business PAYGO system, upgrade the Open Scape Business system to V3 software first and then use on the CLS **re-generate license key** function to receive a valid license file for V3 which has then the "OpenScape Business Info Ready for V3 SW F31505-K158-D129" license. After that, the re-generated license file needs to be activated manually within the OpenScape Business System WBM, under **License management**.

Step by Step

1) Switch to appropriate system operation mode.

Backup of the system taken in one operation mode, cannot be used in another. If for example you take a backup of your system in UC Suite mode, you have to switch the upgraded system in UC Suite mode first before restoring the backup, you cannot restore a backup in UC Smart mode.

V3 mainboard system is operating in UC Smart mode:

The additional Smart VM ports will be created as today, the administrator should delete the configuration from the aforementioned port range on OCC system before the migration takes place.

V3 mainboard system is operating in UC Suite mode:

The additional SmartVM ports will not be created thus the fax configuration will not be affected.

2) Activate the system's license.

CLS Connect	Action
Activated	Regenerate the license to the V3 MAC address on CLS.
Not activated	Import the new license and activate it on the OpenScape Business V2 system. The confirmation code challenge triggers, showing the confirmation cod on the WBM home page.

3) Make a backup of V2 system including the system configuration.

   If the OCC is connected with a Booster Server, a complete backup set from Booster Server is needed to be downloaded and saved.

4) Change the mainboard.

5) Import the new license

CLS Connect	Action
Activated	Import the V3 license file from CLS into the OpenScape Business and the **CLS Connect** will be activated on the V3 mainboard.
Not activated	Generate a new V3 license using the confirmation code on CLS with the V3 mainboard MAC Address, and import the new V3 license file into OpenScape Business.

6) Restore the V2 backup in the V3 mainboard.

7) Change the UC clients IP address configuration.

   At the first connection of UC clients (after migration), please use the new IP address of the V3 mainboard.

Only Fullduplex mode is supported with V3 mainboard.

OptiPoint 4xx/5xx devices are no longer supported with V3 mainboard.

8.12 How to migrate from V2 mainboard to V3 mainboard the master node of a networked system

Prerequisites

The system has a networking license.

Step by Step

1) Upgrade all OpenScape Business slave nodes to V3.

Scenario	Procedure to follow
Upgrade with CLS Connect	Upgrade from V2 to V3 with CLS Connect on page 332

Scenario	Procedure to follow
Upgrade without CLS Connect	Upgrade from V2 to V3 without CLS Connect on page 332

2) Migrate the master node of the system.
   Follow the instruction on How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328

Until the master node is migrated, the slave nodes will be on fail-over mode. After master node migration, they will function fully again.

8.13 How to migrate from V2 mainboard to V3 mainboard the slave node of a networked system

Prerequisites

The system has a networking license.

NOTICE: If CLS Connect is not activated, remove first the slave system from the network on CLS.

Step by Step

1) Migrate the slave system.
   Follow the instruction on How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328
2) Upgrade or migrate the master node.

Scenario	Procedure to follow
Migration from V2 mainboard to V3 mainboard	How to migrate from V2 mainboard to V3 mainboard (standalone system) on page 328
Software upgrade with CLS Connect	Upgrade from V2 to V3 with CLS Connect on page 332
Software upgrade without CLS Connect	Upgrade from V2 to V3 without CLS Connect on page 332

8.14 Migration of HiPath 3000 systems to OSBiz V3 software with V3 mainboard

Software migration is done by the normal HiPath 3000 to OSBiz migration process using Manager E tool. Existing HiPath 3000 ComScendo and S2m licenses are upgraded to the MAC address of the OCCe mainboard. TDM licenses and V3 software indicator are generated by the CLS, based on the XML file information that is created from ManagerE during this procedure.

In case of a reused OCC mainboard from a previous migration of OSBiz to OCCe, no license migration is possible. All licenses need to be purchased.

In case of an OCC from spare parts stock or newly purchased (MAC address is not blocked in CLS), an upgrade of the HiPath 3000 to that MAC address is possible and a new license file is generated (as with migration to OSBiz V2).

8.15 Upgrade from V2 to V3 with CLS Connect

The latest V2R7 is needed to be updated and **CLS Connect** is active. Existing OpenScape Business V2 licenses that are bound to the MAC address of the OCC mainboard are also valid for V3.

After software upgrade, on startup, OpenScape Business V3 software indicates on the CLS that licenses operate in combination with V3 software. V3 information is added into the license file and transferred automatically back into the system via CLS connection during startup. Manual actions are not required.

No action is required in case of software upgrade without migration for slave systems with a networking license. In this case, slave systems can be upgraded and their license will be updated automatically after master system upgrade/ migration.

8.16 Upgrade from V2 to V3 without CLS Connect

Prerequisites

- CLS connect is not active
- OpenScape Business S needs Internet access
- In case of upgrade of a slave node in a networked system, remove first the slave from CLS.

Step by Step

1) Activate the SW-Upgrade license on CLS as a normal license for the OpenScape Business system. Activation on SW-Upgrade license on CLS generates a new license file containing:

   - The new V3 license
   - The new (increased) license file ID
   - If the system is OSBiz S, CLS connect Start is added to the certificate.

2) Import this new license file and activate it to OpenScape Business V2 system.

3) Execute the software upgrade from V2 to V3.

   During start up, after software upgrade to V3, the OpenScape Business system checks the license file and allows licensing functionality only if the V3 license component is available in the license file.

9 Integration into the Internal Data Network (LAN)

The integration of the communication system in the existing internal network (LAN) enables the use of UC solutions and the administration of the communication system on PCs in the internal network.

The following network parameters must be set up in the WBM:

- OpenScape Business X hardware platform: IP address and network mask of the mainboard and the UC Booster Card (if present). These settings are made during the initial installation, but can be changed later.

  Softswitch OpenScape Business S: IP address and subnet mask of the Linux server on which the communication software is running. These settings are made during the Linux installation, but can be changed later.
- The communication system can be optionally set up as a DHCP server (supplied with network-specific parameters such as the subnet mask, default gateway, DNS server) or as a DHCP relay agent. The setup as a DHCP server is performed during the initial installation, but can be changed later. The setup as a DHCP relay agent is performed in Expert mode.
- IP address of the default router and the (external) DNS server for access to other IP networks (e.g., the Internet). These settings are made during the initial installation, but can be changed later.

9.1 LAN Interface

In order to integrate the communication system in the LAN infrastructure, the IP address and internal IP address range of the communication system must be adapted to the IP address scheme of the internal network (LAN).

9.1.1 IP Address and Subnet Mask of the LAN Interface

The IP address and the subnet netmask of the communication system are defined during the initial installation but can also be changed later. You may need to adapt the IP address and/or subnet mask to the IP address range of the LAN.

Hardware Platform

By default, the hardware platform is assigned an IP address and a subnet mask. The UC Booster Card also requires an IP address. The IP address of the UC Booster Card can be configured regardless of whether the UC Booster Card is installed or not.

The hardware platform uses the "LAN" interface of the mainboard for integration into the LAN. Whenever the UC Booster Card is installed, the "LAN" interface of the UC Booster Card must also be connected to the LAN. The hardware platform and UC Booster Card must be located in the same subnet.

To activate the changes to the IP address or subnet mask, a restart of the hardware platform is required.

The changes to the IP address and the subnet mask remain in effect after a software update, but will be reset to the default values in the event of a hardware platform reload. These changes cannot be stored in a backup set.

Softswitch

For a softswitch, the Linux server on which the communication software runs is integrated into the LAN via its network card.

The change of IP address or subnet mask takes effect after a restart of the application (see Restart, Reload, Shutdown).

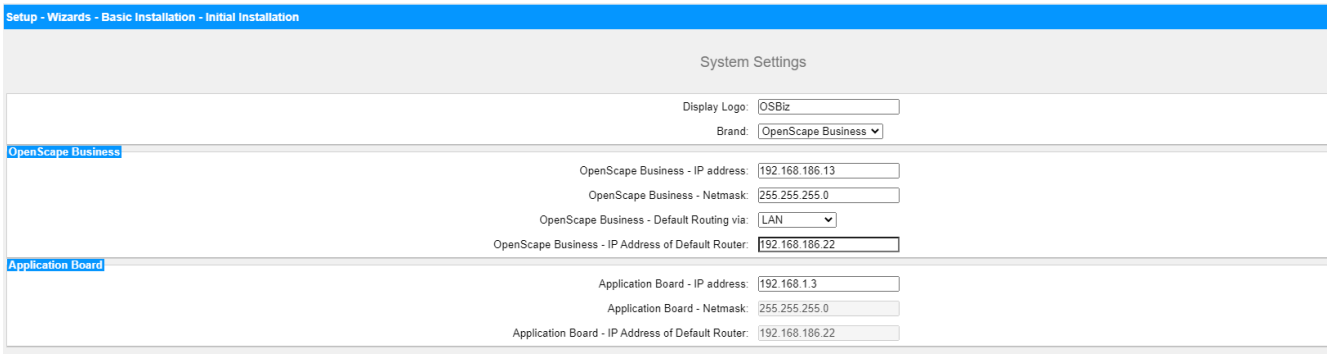
9.1.1.1 How to Change the IP Address and Subnet Mask of the Hardware Platform

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Initial Installation** wizard.



3) Under **OpenScape Business - IP Address**, edit the IP address of the hardware platform. The IP address must conform to the IP address scheme of the internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict. By default, the IP address `192.168.1.2` is entered here.
4) Under **OpenScape Business - Netmask**, edit the subnet mask of the hardware platform. The subnet mask must match the IP address scheme of the internal network. By default, the subnet mask will have been entered as `255.255.255.0`.
5) Click on **OK & Next**.
6) Keep clicking **OK & Next** until you receive a message that the feature has been installed.
7) Click on **Finish**. The hardware platform automatically performs a restart.

9.1.1.2 How to Change the IP Address of the UC Booster Card

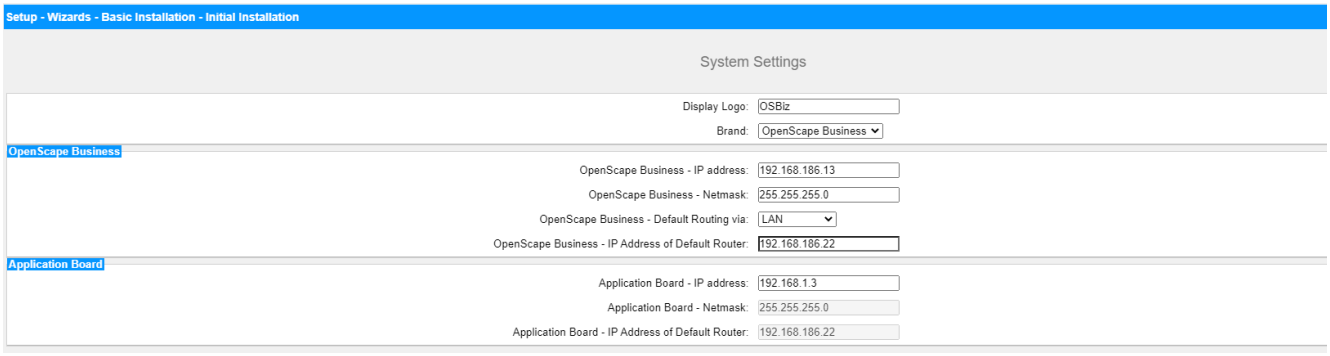
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click on **Edit** to start the **Initial Installation** wizard.



3) Under **UC Booster Card - IP Address**, edit the IP address of the UC Booster Card. The IP address must conform to the IP address scheme of the internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict. By default, the IP address `192.168.1.3` is entered here.
4) Click on **OK & Next**.
5) Keep clicking **OK & Next** until you receive a message that the feature has been installed.
6) Click on **Finish**. The hardware platform automatically performs a restart.

9.1.1.3 How to Check or Change the IP Address and Subnet Mask of the Softswitch

Step by Step

1) Click on **Computer** in the task bar.
2) In the menu tree, click on **System** > **YaST**.
3) Enter the password for the root user and click **Continue**. The YaST Control Center is opened.
4) Click on **Network Devices** in the menu tree.
5) In the **Network Devices** area, click on **Network Settings**.
6) Select the desired network card in the **Overview** window and click on **Edit**.
7) Enable the radio button **Statically assigned IP Address**.
8) Under **IP Address**, change the IP address of the Linux server on which the software of the softswitch is running. The IP address must conform to the IP address scheme of the internal network and must not have been assigned to any network client, since this would otherwise result in an IP address conflict.
9) Under **Subnet mask**, edit the subnet mask of the Linux server. The subnet mask must conform to the IP address scheme of the internal network.
10) Click on **Next** followed by **OK**.
11) Close the **YaST Control Center**.

9.1.2 Internal IP Address Range of the LAN Interface

The internal IP address range of the LAN interface that is used by the hardware platform for the internal communication of its modules can be changed if necessary.

The hardware platform uses the internal IP address range 192.168.3.xxx by default. This address range can also be edited and set to a desired IP address range. The internal subnet mask is 255.255.255.0 and cannot be changed.

To activate the changes to the internal IP address range, a restart of the hardware platform is required.

The changes to the internal IP address range remain in effect with a software update, but will be reset to the default values in the event of a reload. These changes cannot be stored in a backup set.

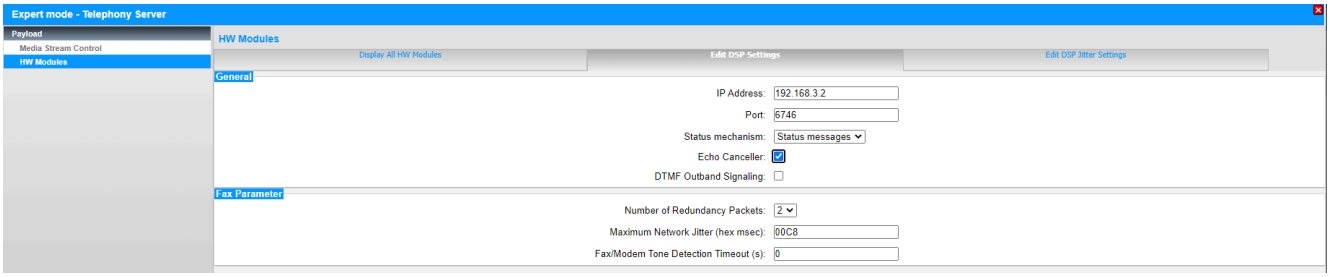
9.1.2.1 How to Change the Internal IP Address Range of the Hardware Platform

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Payload**.
3) Click **Hardware Modules** in the menu tree.
4) Click on the **Edit DSP Settings** tab.



5) In the **General** area under **IP address**, enter an IP address for the communication system that is in the desired new internal range, e.g., `192.168.40.2`. The entire IP address range (in this example `192.168.40.xxx`) is now blocked for other clients on the LAN.
6) Click on **Apply** and confirm with **OK**.

9.1.2.2 How to Reset the Internal IP Address Range of the Hardware Platform

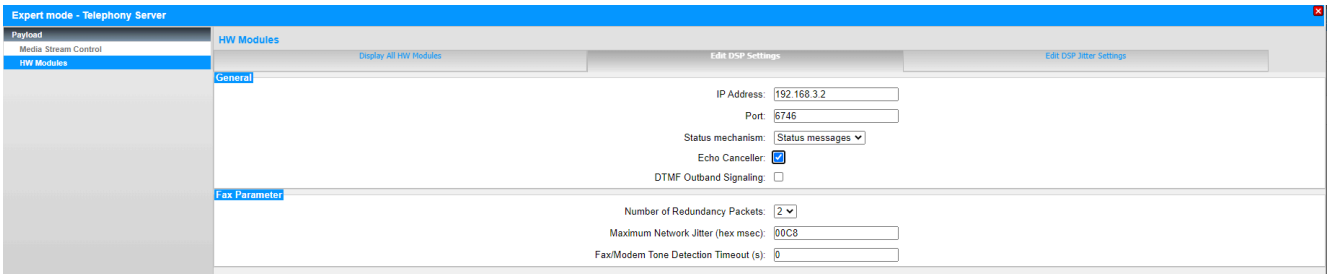
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Payload**.
3) Click **Hardware Modules** in the menu tree.

4) Click on the **Edit DSP Settings** tab.



5) In the **General** area, enter the IP address `192.168.3.2` under **IP address**. The entire IP address range (`192.168.3.xxx`) is now blocked for other clients on the LAN.
6) Click on **Apply** and confirm with **OK**.

9.2 DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that enables the dynamic allocation of network-specific data to the IP stations of a network (e.g., a LAN) with the aid of a DHCP server.

DHCP thus makes it possible to automatically integrate IP stations (e.g., IP phones or PCs) in an existing LAN. The IP station must be configured to automatically receive the network-specific data and is thus a DHCP client. The DHCP server provides the IP stations with the network-specific data on request.

9.2.1 DHCP Relay Agent

When using the internal DHCP server of the hardware platform, the internal DHCP server and the DHCP clients must be on the same network segment. If this is not the case, the hardware platform must be configured as a DHCP relay agent. The DHCP requests of the IP stations are then forwarded from the hardware platform to the actual DHCP server.

9.2.1.1 How to Configure the Hardware Platform as a DHCP Relay Agent

If the hardware platform is configured as a DHCP relay agent, it relays DHCP requests on to the external DHCP server.

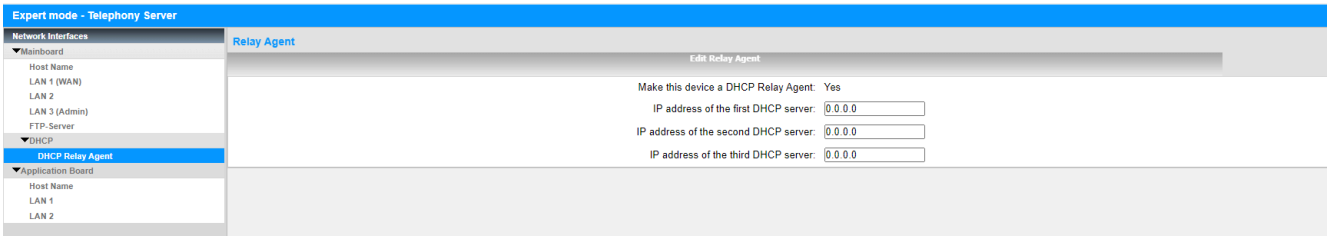
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony Server** > **Network Interfaces** in the navigation tree.
3) Click on **Mainboard** > **DHCP** in the menu tree.
4) Enable the **DHCP Relay Agent** radio button.
5) Click on **Apply** and confirm with **OK**.

6) Click **DHCP Relay Agent** in the menu tree.



7) Enter the **IP address of the first DHCP server**.

8) Enter the **IP address of the second DHCP server**.

9) Enter the **IP address of the third DHCP server**.

INFO: You can enter up to three DHCP servers. The entry of the first DHCP server is mandatory.

---

10) Click on **Apply**, followed by **OK**.

9.2.2 DHCP Server

The DHCP server assigns network-specific information such as the IP address and subnet mask of the IP station, the IP address of the default gateway, the IP address of the SNTP server, etc., dynamically to the IP stations (i.e., the IP phones, SIP phones, PCs, WLAN access points, and so on).

The internal DHCP server of the communication system or an external DHCP server can be used as DHCP server (e.g., the DHCP server of the Internet router).

In the hardware platform, the integrated DHCP server is enabled by default. If an external DHCP server is to be used, the internal DHCP server must be disabled. Otherwise, conflicts may arise with the external DHCP server.

For the softswitch, the Linux server can be configured as an internal DHCP server.

The decision as to whether the internal DHCP server of the communication system or an external DHCP server is to be used should be made during the initial startup. The internal DHCP server can also be enabled or disabled later. Even the network-specific data can be configured later.

Internal DHCP Server

If the internal DHCP server is used, the IP stations are automatically supplied with the following network-specific data:

- IP address and subnet mask of the IP station
- IP address of the communication system (default gateway)
- IP address of the SNTP server (to obtain the date and time)
- IP address of the DNS server (for name resolution)
- IP address of the SIP server (for the authentication of SIP stations)
- IP address of the internal DLI or the external DLS server (for the software update of the IP system phones)
- Routing rules

External DHCP Server

If an external DHCP server is used, it must support a vendor-specific option space to enable the provision of vendor-specific parameters. The following network-specific data should be entered in the external DHCP server:

- IP address and subnet mask of the IP station
- IP address of the default router = Option 3
- IP address of the communication system (default gateway) = Option 33
- IP address of DNS server (for name resolution) = Option 6
- IP address of the internal DLI or the external DLS server (for the software update of the IP system telephones) = Option 43
- Only for SIP phones: IP address of the SIP server (SIP registrar, for the authentication of SIP stations) = Option 120
- Only for SIP phones: IP address of the SNTP server (to supply the SIP phones with the date and time) = Option 42

NOTICE: Additional information on DHCP server in a Windows environment can be found here: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

If no such entries can be made at the external DHCP server, this data must be entered directly at the IP system phones. Only then can the IP system phones be automatically supplied with the current date and time and the latest software updates, for example.

For further information please refer to the following Unify Experts Wiki page under: http://wiki.unify.com/wiki/DHCP

DHCP Address Pool (IP Address Ranges)

Whenever an IP station logs in at the DHCP server, it receives, among other things, a dynamically assigned IP address. The administrator can optionally define an IP address range from which the DHCP server can assign IP addresses to the IP stations. In this case, for example, not all IP addresses from the range 192.168.1.xx are to be assigned, but only those from 192.168.1.50 to 192.168.1.254, since the lower IP addresses up to 192.168.1.49 are to be reserved for IP stations with static IP addresses.

In fact, even multiple IP address ranges can set up for the internal DHCP server under **Network Interfaces** in expert mode.

9.2.2.1 How to Enable and Configure the DHCP Server of the Hardware Platform

The **Network Configuration** wizard can be used to enable and configure the DHCP server of the hardware platform.

Prerequisites

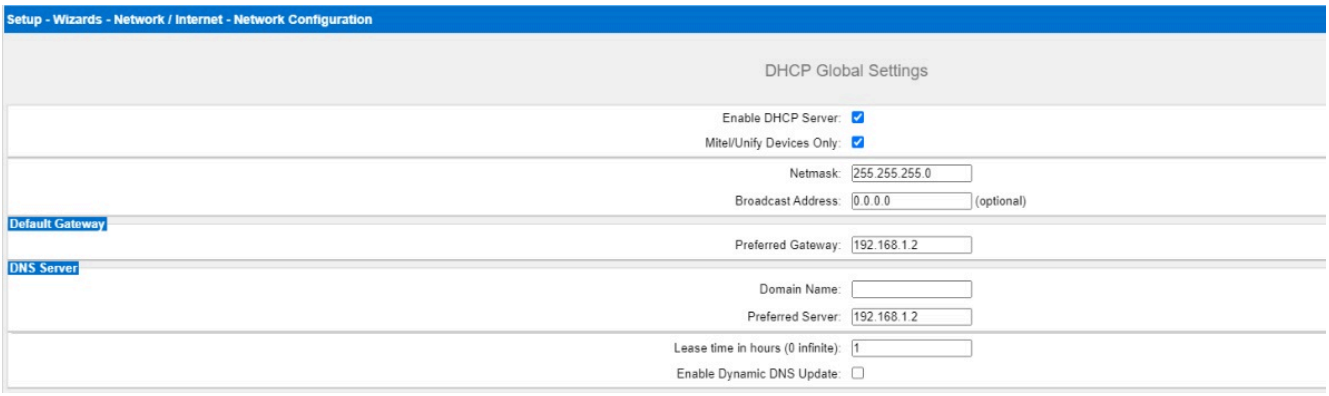
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Network/Internet**.

3) Click on **Edit** to start the **Network Configuration** wizard.



4) Check the **Enable DHCP Server** check box.
5) If needed, enable the **Mitel/Unify Devices Only** checkbox.

NOTICE: This option is only available for V3 mainboards.

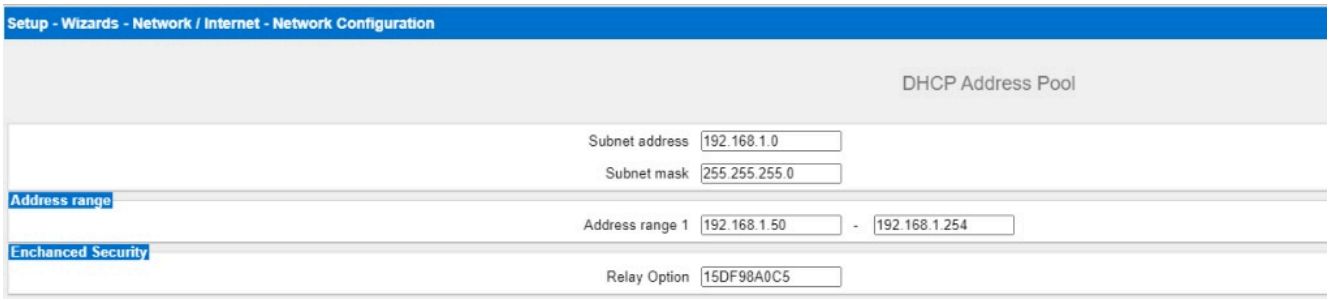
---

6) Enter the subnet mask of your network in the **Subnet Mask** field (e.g., `255.255.255.0`).
7) In the **Broadcast Address** field, enter the Broadcast address ("last" IP address of the net or subnet, default: `0.0.0.0`) if required.
8) In the field **Preferred Gateway**, enter the IP address of the default gateway. As a rule, the IP address for the Internet router is usually `192.168.1.1`.
9) If you need a fully qualified domain name for the DHCP server, enter this under **Domain Name** (max. 80 characters).
10) In the field **Preferred Server**, enter the IP address of an available DNS server, e.g., the IP address of the Internet router, `192.168.1.1`.
11) If required, enter the maximum lease time in hours (default: 1 h, 0 = infinite lease time) in the field **Lease Time in hours (0 = infinite)**.
12) If you want to permit dynamic updates of the DNS server, enable the option **Enable Dynamic DNS Update** (default: disabled).

NOTICE: If Dynamic DNS Update option is enabled, it is mandatory to configure **Domain Name** in IP Address Pool respective Domain name field.

---

13) Click on **OK & Next**. The settings for the DHCP address pool are displayed.



14) In the **Subnet Address** field, enter the lowest IP address of the subnet in which the desired IP address range is located (in our example, `192.168.1.0`).
15) Enter the subnet mask of the desired IP address range in the **Subnet Mask** field (e.g., `255.255.255.0`).
16) Enter the upper and lower threshold for the desired IP address range in the **Address Range 1** field (e.g., `192.168.1.50` to `192.168.1.254`).
17) If needed, specify the value of the **Relay Option** field.

NOTICE: This option is only available for V3 mainboards.

---

18) Click on **OK & Next**. The **Routing Settings** window appears.
19) In the field **IP Address of DNS Server**, enter the IP address of an available DNS server, e.g., the IP address of the Internet router, `192.168.1.1`.
20) Select the item **LAN** from the **Default Routing via** drop-down list.
21) If access to the Internet occurs via an Internet router, enter the IP address of the Internet router (e.g., `192.168.1.1`) in the **IP address of Default Router** field.
22) Click on **OK & Next** followed by **Finish**.

9.2.2.2 How to Disable the DHCP Server of the Hardware Platform

The **Network Configuration** wizard can be used to deactivate the DHCP server of the hardware platform.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network/Internet**.
3) Click on **Edit** to start the **Network Configuration** wizard.
4) Clear the **Enable DHCP Server** check box.
5) Keep clicking **OK & Next** until you receive a message that the feature has been installed.
6) Click on **Finish**.

9.2.2.3 How to Enable and Configure the DHCP Server of the Softswitch

Step by Step

1) Click on **Computer** in the task bar.
2) In the menu tree, click on **System** > **YaST**.
3) Enter the password for the root user and click **Continue**. The YaST Control Center is opened.
4) Click on **Network Services** in the menu tree.
5) In the **Network Services** area, click on **DHCP Server**.

6) Mark the desired network card and click **Select**.
7) Select the **Open Firewall for Selected Interfaces** check box.
8) Click on **Next**.
9) If you need a fully qualified domain name for the DHCP server, enter this under **Domain Name** (max. 80 characters).
10) In the field **Primary Name Server IP**, enter the IP address of an available DNS server, e.g., the IP address of the Internet router, `192.168.1.1`.
11) In the field **Default Gateway (Router)**, enter the IP address of the default gateway. As a rule, the IP address for the Internet router is usually `192.168.1.1`.
12) Enter the SNTP server configured during initial setup in the **NTP Time Server** field.
13) Click on **Next**.
14) Enter the lower limit of the desired IP address range in the field **First IP Address** and its upper limit in the field **Last IP Address** (e.g., `192.168.1.50` to `192.168.1.254`).
15) Select the **Allow Dynamic BOOTP** check box.
16) Click on **Next**.
17) Enable the **When Booting** radio button.
18) Click on **Finish**.
19) Close the **YaST Control Center**.

9.2.2.4 How to Disable the DHCP Server of the Softswitch

Step by Step

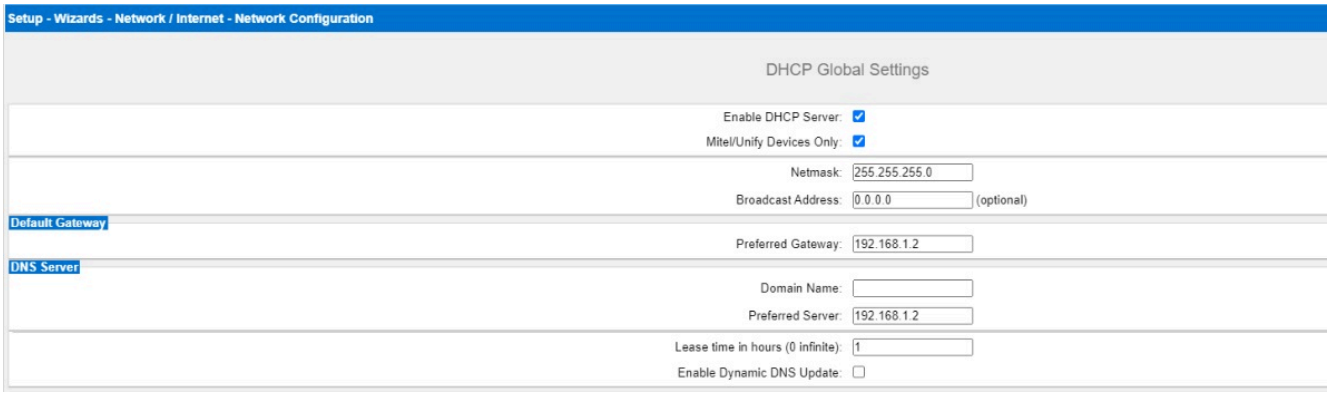
1) Click on **Computer** in the task bar.
2) In the menu tree, click on **System** > **YaST**.
3) Enter the password for the root user and click **Continue**. The YaST Control Center is opened.
4) Click on **Network Services** in the menu tree.
5) In the **Network Services** area, click on **DHCP Server**.
6) Clear the **Start DHCP Server** check box.
7) Click on **Finish**.
8) Close the **YaST Control Center**.

9.2.2.5 How to Enable DHCP for Mitel/Unify Devices Only

This option allows the system administrator to activate the OpenScape Business DHCP service exclusively for Mitel and Unify devices.

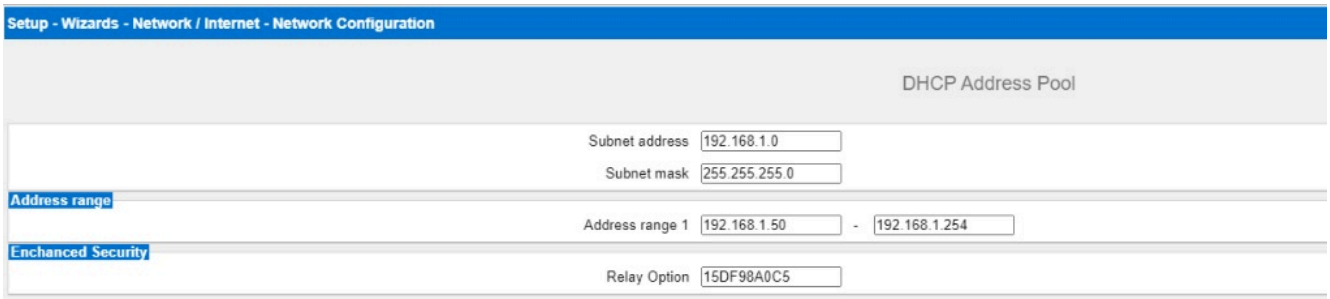
Prerequisites

You are in the **DHCP Global Settings** window.



Step by Step

1) Leave the **Enable DHCP Server** check box enabled.
2) Click to enable the **Mitel/Unify Devices Only** checkbox. See DHCP Server > Global Parameters for further information on this option.
3) Go to the **Netmask** field and adjust the subnet mask to your IP address range (for example, `255.255.255.0`).
4) In the field **Preferred Gateway**, enter the IP address of the Internet router (e.g., `192.168.1.1`).
5) In the field **Preferred Server**, enter the IP address of the DNS server (e.g., the IP address of the Internet router, `192.168.1.1`.
6) Click on **OK & Next**. The **DHCP Address Pool** window appears.



7) Specify the values for **Subnet address**, **Subnet mask** and **Address range 1** to define the IP address range to be managed by the internal DHCP server.

   If the internal network uses static IP addresses (e.g., for a printer server), the IP address range (DHCP address pool) must be selected so that the fixed IP addresses are not included within this range.

   Example:

   Internet router: `192.168.1.1`

   OpenScape Business: `192.168.1.2`

   UC Booster Card: `192.168.1.3`

   Subnet address: `192.168.1.0`

   Subnet mask: `255.255.255.0`

   Printer Server: `192.168.1.10`

   DHCP address pool: `192.168.1.50` to `192.168.1.254`

8) Specify the value of the **Relay Option** field.
9) Click on **OK & Next**.

Next steps

Configure country and time settings.

9.3 DNS - Name Resolution

The Domain Name Service (DNS) serves to the translate names to numerical addresses. This enables host names or domain names to be converted to IP addresses, and vice versa.

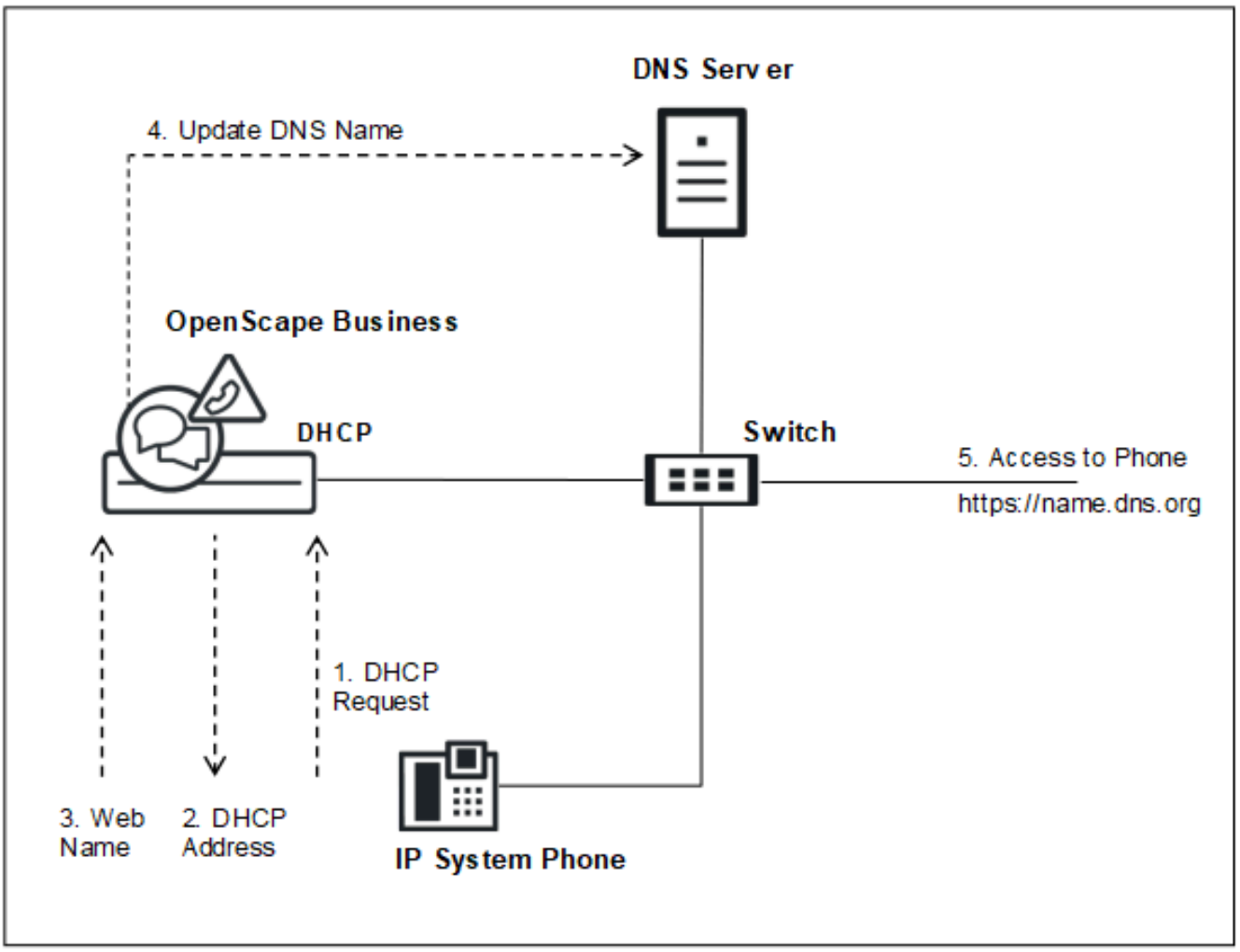
The DNS uses a hierarchical database that manages the Internet name space and is distributed over a collection of servers worldwide. This name space is divided into so-called zones (domains). Separate Internet-independent DNS servers are usually operated for local requirements – for example, within a corporate network.

Name Resolution for IP System Phones

The following prerequisites must be met:

- Windows 2008 DNS Server (with the current patch level and the "Allow unsafe update" setting enabled)
- The internal DHCP server is enabled
- The "Enable Dynamic DNS Update" functionality is activated in the internal DHCP server (see DHCP Server)
- The web name is entered in the IP system telephone.

The IP system telephone sends a DHCP request (1) and receives a valid IP address and other network-specific data (2) from the internal DHCP server. After receiving this data, the IP system telephone sends the set web name to the internal DHCP server (3), which then forwards the name automatically to the configured DNS server (4). The DNS server now knows the name associated with the IP address of the IP system telephone. The IP system telephone can now be accessed via the WBM by using its web name (5).



DNS Server

The DNS server, also called a name server, is a program that responds to requests about domain names or computer names. Even the PC on which this program runs can be designated as a DNS server.

For requests about a domain name or a host name, the DNS server returns the corresponding IP address.

Example: for `www.wikipedia.org`, DNS server on the Internet will return the IP address `91.198.174.2`.

If the preferred DNS server cannot answer a request, it forwards the request to another DNS server.

For a softswitch, the Linux server on which the communication software runs can be configured as a DNS server. The hardware platform cannot be used as a DNS server. An external DNS server can be specified for both the softswitch as well as the hardware platform.

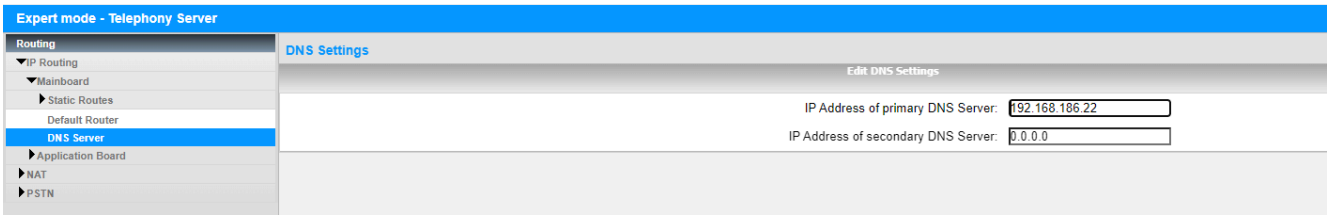
9.3.1 How to Define an External DNS Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Routing**.
3) Navigate in the menu tree to **IP Routing** > **Mainboard** > **DNS Server**. The **Edit DNS Settings** window appears.



4) Enter the IP address of the relevant external DNS server in the field **IP Address of DNS Server**.
5) Click on **Apply** followed by **OK**.

NOTICE: In case of an OpenScape Business S system, a system reboot is necessary in order the changes to be applicable.

9.4 IP Routing

In data technology, IP routing describes the definition of paths (routes) for data streams within networks. IP routing is required when the sender and recipient are on different networks.

Default Router

To ensure that IP stations can also reach destinations outside their own networks that are not explicitly listed in a route table, a gateway must be specified for forwarding packets of this kind (default router). The default router will then redirect the data to the parent network.

You can enable or disable IP routing via a default router for both the mainboard and the Application Board.

Static Routes

Static routes are used to establish the path along which data will travel to a network that cannot be reached via the default router.

You can create static routes for both the mainboard and the Application Board.

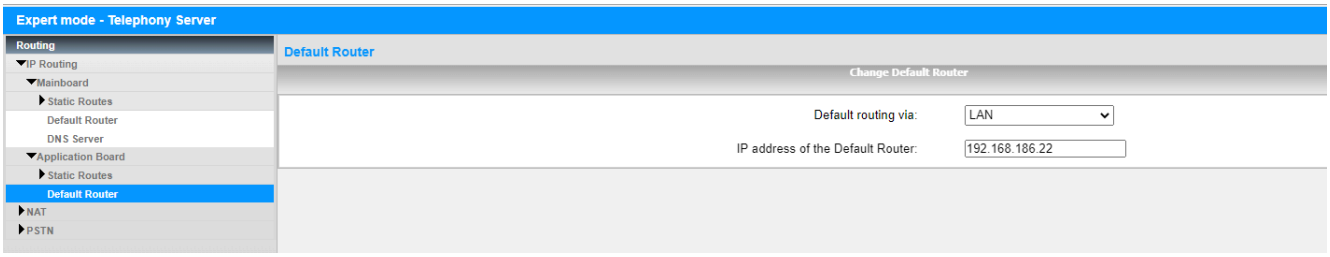
9.4.1 How to Activate or Deactivate the Default Router

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Routing**.
3) Navigate in the menu tree to **IP Routing** > **Mainboard / Application Board** > **Default Router**. The **Edit Default Router** window appears.



4) If you want to enable IP routing over a default router, select the entry **LAN** in the **Default Routing via** list box and enter the IP address of the default router e.g., the IP address of the Internet router **192.168.1.1** under `IP Address of Default Router`.
5) If you want to disable IP routing over a default router, select the entry **No interface** in the **Default routing via** list box.
6) Click on **Apply** followed by **OK**.

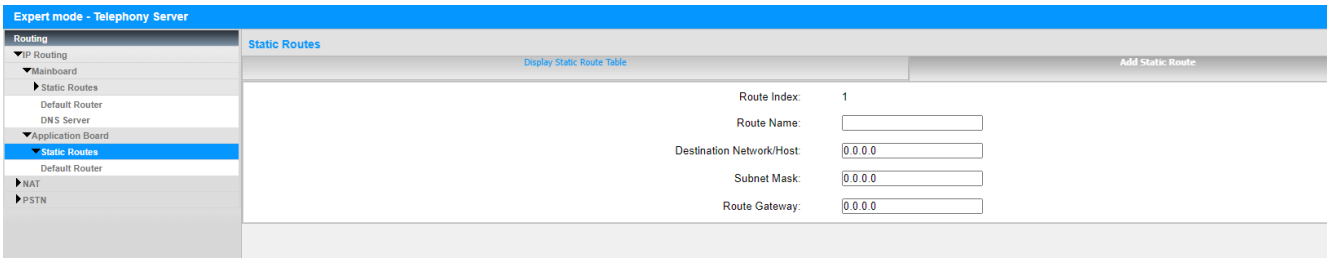
9.4.2 How to Add a Static Route

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Routing**.
3) Navigate in the menu tree to **IP Routing** > **Mainboard / Application Board** > **Static Routes**. The **Static Routes** window is displayed.
4) Click on the **Add Static Route** tab. The **Route Index** shows which route is added.



5) Enter the required name for this route in the **Route Name** field.
6) Enter the IP address of the **Destination Network/Host**.

7) Enter the IP address of the **Destination Subnet Mask** (subnet mask).
8) Enter the IP address of the router you want to use to reach the destination network in the **Route Gateway** field.
9) If you have created one or more static routes for the mainboard, you can copy all static routes of the mainboard to the Application Board with the **Copy to OCAB** button.
10) Click on **Apply** followed by **OK**.

9.4.3 How to Delete Static Routes

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Routing**.
3) Navigate in the menu tree to **IP Routing** > **Mainboard / Application Board** > **Static Routes**.
4) Mark the route you want to delete.
5) Click the **Delete Static Route** tab.
6) Click on **Delete**.
7) Confirm the advisory message and then click **OK**.

9.5 Deployment Service (DLS and DLI)

DLI and DLS can be used to manage IP components centrally and to deploy their software. The DLI is integrated in the communication system. The DLS is a standalone application which must be installed on an external server PC.

DLI (Deployment Server Integrated)

The DLI is a component which is integrated in the communication system and provides limited DLS functionality. The internal DLI can be used to centrally configure all IP system phones connected to the communication system and to equip them with the latest phone software. For DeskPhone CP 400/600/600E/700/700X/710, when DLI is enabled, the following UC Server parameters are automatically configured: UC Protocol, UC Server address, UC Server port.

The internal DLI also works with the integrated FTP server on which the latest phone software is stored.

If the IP address of the DLI is known to the DHCP server, the DHCP server sends this data to the IP system telephone (HFA, SIP) as soon as the phone logs into the internal network. This enables the telephone to retrieve the current software from the FTP server of the communication system. The DLI is configured by default in the internal DHCP server. If an external DLS server is to be used instead, its IP address must be configured in the internal DHCP server.

DLS (Deployment Service)

The DLS is a client/server application for the central administration of the IP components. The DLS server is not integrated in the communication system and must be installed on a server PC. The DLS client runs on the IP components. Administration occurs via a web browser.

IP components can be IP system phones, SIP phones, SIP clients and IP gateways.

NOTICE: The properties and features of the DLS can be found in the product description of the DLS and are not described in this documentation.

DLI or DLS with External DHCP Server

In order to ensure that the software of IP system telephones (HFA, SIP) can be updated automatically even when using an external DHCP server, you have the following alternatives:

- Configure the IP address of the DLI or DLS in the external DHCP server

  When using an external DHCP server, the network-specific data and the IP address of the external deployment server (DLI or external DLS server) must be entered. In addition, the latest phone software must be stored on the external DLS server.
- Configure all system phones

  The IP address of the deployment server must be entered as the DLS address for each IP system phone (IP address of the communication system for the internal DLI or IP address of the external DLS server).

Features and Restrictions

Function	DLI	DLS
Central configuration of the parameters of IP components The parameters of the IP components can be configured via customizable XML templates.	yes	yes
Plug&Play commissioning of the IP components Using a DHCP server, the IP components can log into the system automatically after being connected to the system for the first time or after an IP component is replaced, for example.	Yes	Yes
Central and automatic software update for IP components Whenever a new software version is available, the IP components are automatically supplied with the latest version of the software the first time the user logs on. The IP address of the DLI/DLS must be configured in the IP component.	Yes	Yes The latest phone software must be stored on the DLS.

Function	DLI	DLS
Centralized inventory management of IP components The data on the hardware configurations of the IP components can be accessed and retrieved centrally.	no	Yes
Support for IP Mobility (Desk Sharing) The telephony data of a user (e.g., program keys, directory entries, journals) is stored centrally and can be retrieved at other phones).	Yes Not for SIP phones, Not possible in the internetwork.	Yes Not for SIP phones, In homogeneous networks (only OpenScape Business systems), only with closed numbering, Not in heterogeneous networks (with OpenScape 4000 or OpenScape Voice).
SPE support in networks	SPE in networks is possible. DLS has to be used (no DLI).	Yes The keys and certificates to be deployed must be available on the DLS.
Central supply for several different platforms	no	Yes
Activation of the 2nd LAN interface of IP system phones (PC Ethernet mode). See Basic Settings > Phone Parameter Deployment	Yes	Yes

Deployment- und Licensing Client (DLSC)

To use DLS functions such as the element manager, for example, the communication system must allow the external DLS to access the configuration data. The communication system is then operated as Deployment and Licensing Client.

9.5.1 How to Configure the External DLS Server in the Internal DHCP Server

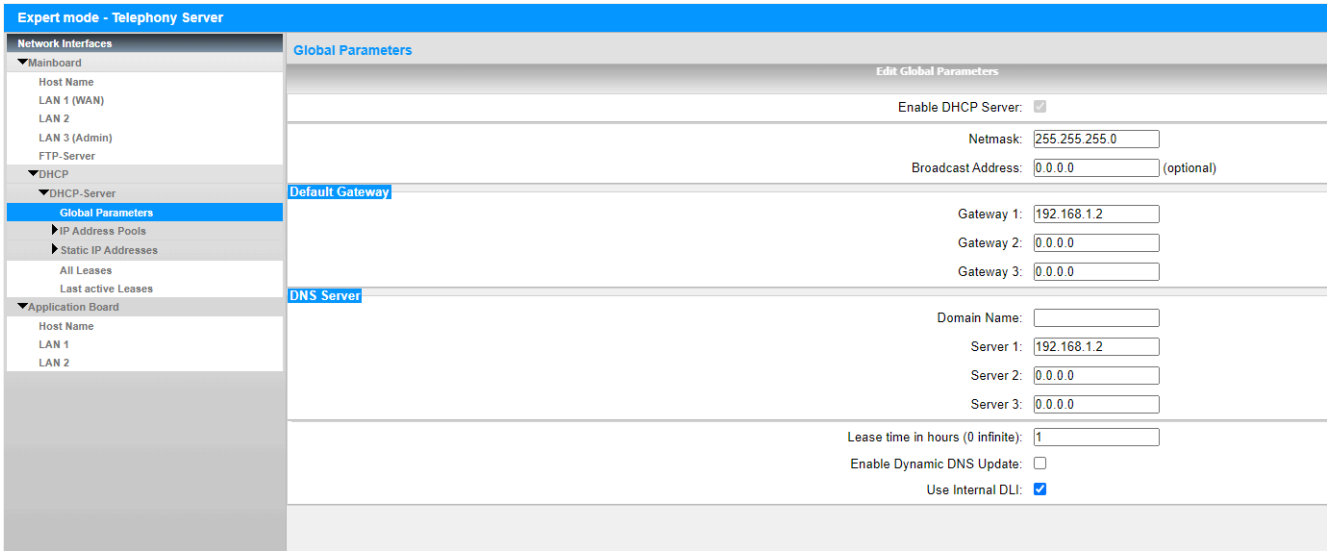
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony Server** > **Network Interfaces** in the navigation tree.

3) Navigate in the menu tree to **Mainboard** > **DHCP** > **DHCP Server** > **Global Settings**. The **Edit Global Parameters** window is displayed.



4) Clear the **Use Internal DLI** check box.
5) Enter the IP address at which the server can be reached in the **IP Address** field.
6) Enter the port used by the DLS server in the **Port** field. This port must be enabled in the firewall.
7) Click on **Apply**, followed by **OK**.

9.5.2 How to Enable the Internal DLI

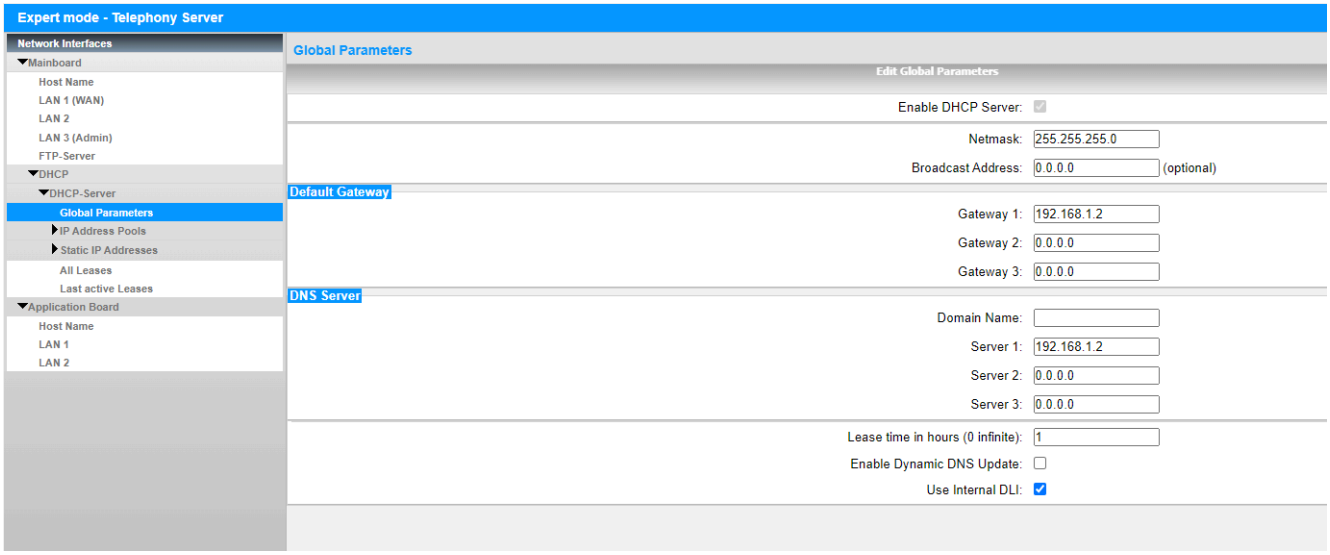
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony Server** > **Network Interfaces** in the navigation tree.

3) Navigate in the menu tree to **Mainboard** > **DHCP** > **DHCP Server** > **Global Settings**. The **Edit Global Parameters** window is displayed.



4) Enable the **Use Internal DLI** check box. This check box is enabled by default.
5) Click on **Apply**, followed by **OK**.

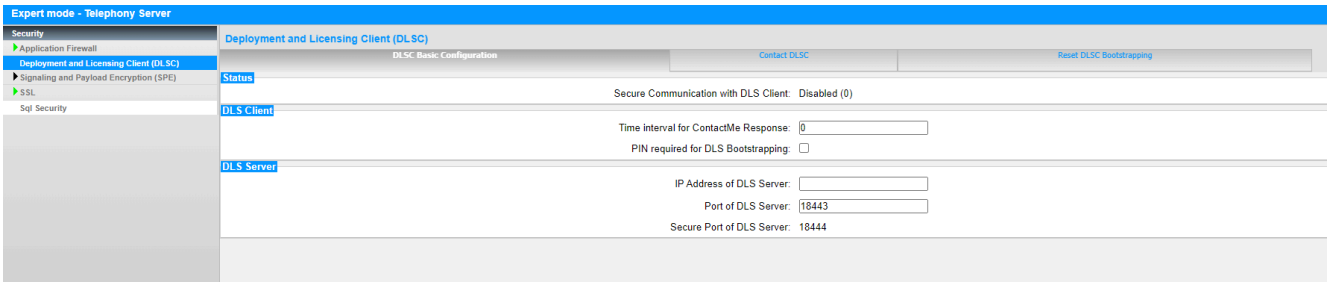
9.5.3 How to Configure the Communication System as a Deployment and Licensing Client

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Security**.
3) Click **Deployment and Licensing Client (DLSC)** in the menu tree.



4) On the **DLSC Basic Configuration** tab in the **DLS Server** area, enter the IP address at which the external DLS server can be reached in the **IP Address of DLS Server** field.
5) Enter the port used by the DLS server in the **Port of DLS Server** field. The two displayed ports must be enabled in the firewall.
6) Click on **Apply** followed by **OK**.

10 Connection to Service Provider

The communication system supports connection to public communication networks. The connection to the IP network provides access to the Internet and Internet telephony, ane the connection to the Central Office provides access to the ISDN network and the analog network.

Access to the Internet occurs via either an Internet modem or an Internet router.

ISDN trunk access for the hardware platforms occurs via the mainboard or additional plug-in boards. ISDN trunk access is not possible with the softswitch.

The analog trunk access for the hardware platforms requires an additional plug-in board. Analog trunk access is not possible with the softswitch.

10.1 Internet Access

A broadband connection (DSL or connection) is required for access to the Internet. This enables fast data transfers within the framework of the available bandwidth.

Internet Access via a DSL Connection

Conventional telephone lines are used for broadband Internet access via DSL (digital subscriber line). The Internet access can be used at the same time as the normal phone. Fax, analog phone or ISDN are also available during the DSL connection. This makes it possible to implement Internet access that is permanently available as in the case of a dedicated line (flat rate).

For Internet access via DSL, you need a modular jack (analog or ISDN) and an Internet Service Provider (ISP). The ISP provides a splitter and an Internet modem (DSL modem) or an Internet router with a built-in Internet modem. The splitter divides the signal into DSL and telephony parts and forwards the DSL signals to the Internet modem.

The communication system can be connected directly to the Internet modem or to the Internet router with an integrated Internet modem. In the first case, the access data of the ISP must be entered in the communication system; in the second, the Internet router must be made known to the communication system. The access data of the ISP is saved in the Internet router.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

Internet Access via a Cable Connection

The broadband connection to the Internet is implemented via the TV cable. In addition to transmitting TV signals, the TV cable connection can be used for accessing the Internet and making calls. This means you do not need a telephone line to surf and for telephony.

For Internet access via cable, you need a cable provider that offers this feature. The cable provider is also your Internet Service Provider (ISP). This cable provider supplies you with a cable port with a back channel and a cable modem that transmits the data over the TV cable network. The cable port and the communication system are connected to the cable modem over Ethernet. Internet data filtration takes place directly in the cable modem.

The communication system can be connected directly to the cable modem or to an Internet router that is connected to the cable modem. In both cases, the cable modem or the Internet router must be made known to the communication system.

To use Internet telephony, you will also need an Internet Telephony Service Provider (ITSP, SIP provider).

Configuring Internet Access

The configuration of Internet access in the WBM depends on whether the Internet connection has already been set up in an external router or whether it occurs via an Internet modem and thus needs to be set up in the WBM.

- **Internet access through an Internet modem** (**DSL at WAN port directly**)

  You want to operate the communication system directly at an Internet modem (DSL, cable, UMTS ...). OpenScape Business has the Internet router integrated. Enter the access data of the Internet Service Provider (ISP) directly in the communication system and use the WAN port of the communication system. This option is not available with the softswitch.



You have the following options:

– Internet access via a preconfigured ISP
– Internet access via the standard ISP PPPoE
– Internet access via the standard ISP PPTP

If your ISP is not listed under the preconfigured ISPs, use the default ISP PPPoE or PPTP.

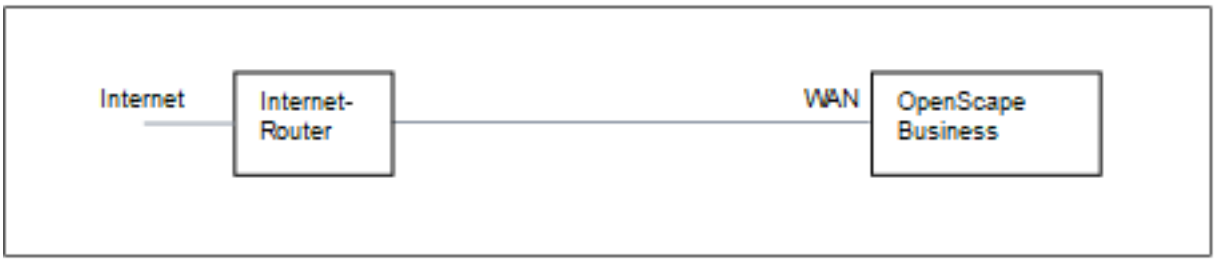
- **Internet access via an external Internet router**

  You want to operate the communication system at an external Internet router. The Internet Service Provider is already configured in the Internet router.

  You have the following options:

  – **Internet access via an external Internet router at the WAN port**

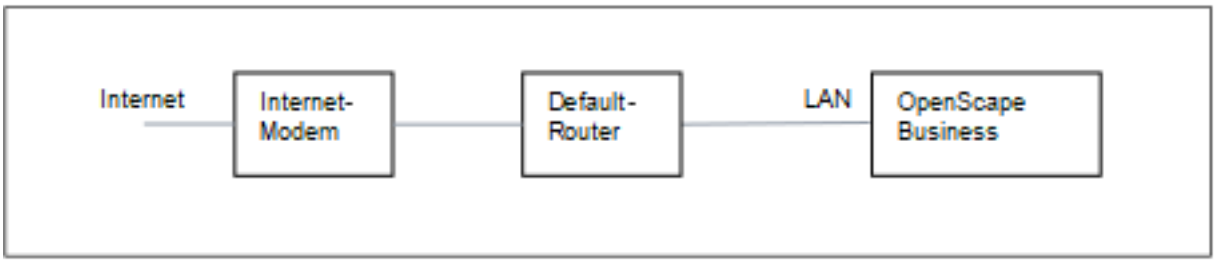
    (**TCP/IP at WAN port via an external router**)



    To do this, you use the WAN port of the communication system. OpenScape Business either knows the Internet router or works as a DHCP client. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

  – **Internet access via an external Internet router at the LAN port**

    (**TCP/IP at LAN port via an external router**)



    To do this, you use the LAN port of the communication system. OpenScape Business knows only the default router and not the underlying infrastructure. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.

- **Disable Internet access** (default setting)

  You do not want to use the Internet. Then leave the Internet access disabled.

10.1.1 Internet Access via an External Internet Router

The **Internet Configuration** wizard helps you configure your Internet access via an additional Internet router.

To set up Internet access, you have the following options:

- **Internet access via an external Internet router at the LAN port**

  To do this, you use the LAN port of the communication system. To activate the connection to the Internet router, the IP address of the default router and that of the DNS server must be made known to the communication system.

- **Internet access via an external Internet router at the WAN port**

  To do this, you use the WAN port of the communication system. This option can be used if the Internet router is located in another network segment and has its own DHCP server.

10.1.1.1 How to Configure Internet Access via an External Internet Router over the LAN Port

The **Internet Configuration** wizard helps you configure the Internet access if the communication system is operated downstream of an additional Internet router. The communication system and the Internet router are in the same LAN segment. You must enter the IP address of the Internet router and the DNS server for this.

Prerequisites

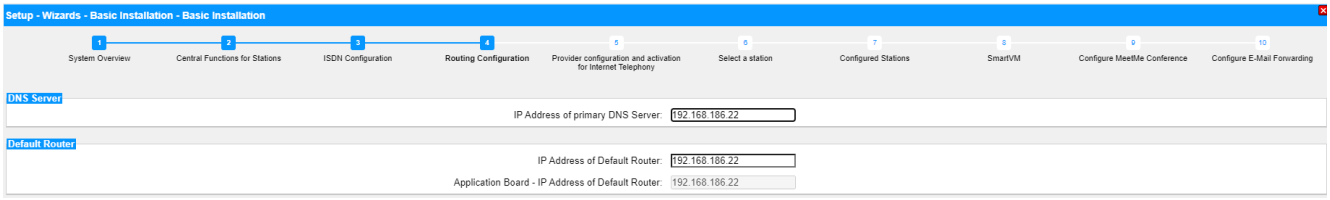
You are logged on to the WBM with the **Advanced** profile.

For OpenScape Business X: The communication system is connected to the customer network via the "LAN" port. The "WAN interface must not be used for this purpose.

For OpenScape Business S: The Linux server is connected to the customer network via the LAN interface of the network card.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click on **Edit** to start the **Internet Configuration** wizard.
4) Disable the **No Internet Access** check box.
5) Activate the radio button **TCP/IP at LAN Port via an external router** and click on **OK & Next**.



6) Enter the IP address of the local DNS server (e.g., the Internet router) or the Internet DNS server (for Internet telephony, for example) in the **IP Address of DNS Server** field.
7) Enter the IP address of the external Internet router in the **IP Address of Default Router** field.
8) Click on **OK & Next** followed by **Finish**.

10.1.1.2 How to Configure Internet Access via an External Internet Router over the WAN Port

The **Internet Configuration** wizard helps you configure the Internet access if the communication system is operated downstream of an additional Internet

router. The communication system and the Internet router must not be located in the same LAN segment.

Prerequisites

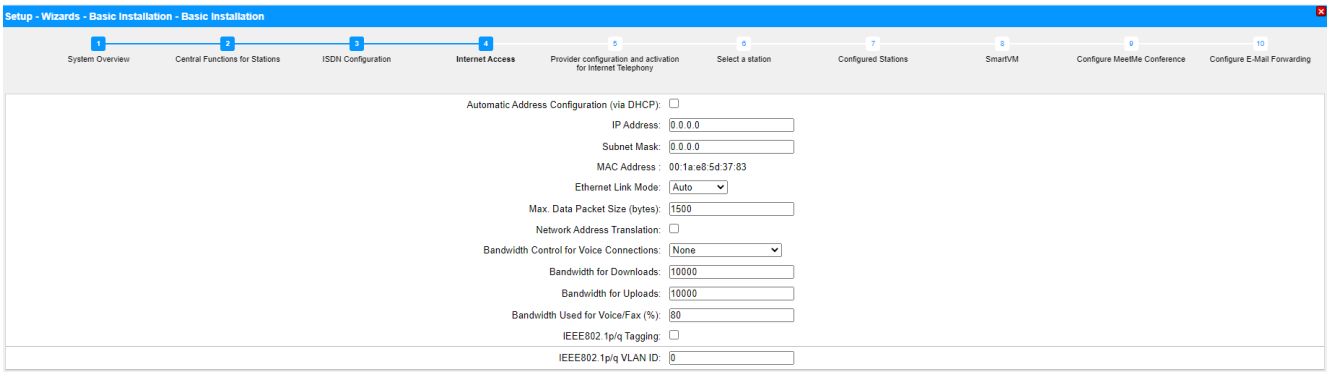
You are logged on to the WBM with the **Advanced** profile.

The communication system must be connected to the LAN segment of the customer network in which the Internet router is located via the "WAN" interface.

You are in the **Configure Internet Access** window.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click on **Edit** to start the **Internet Configuration** wizard.
4) Disable the **No Internet Access** check box.
5) Activate the radio button **TCP/IP at WAN Port via an external router** and click **OK & Next**.



6) If the network-specific data for the WAN interface are to be obtained from an already active DHCP server:
   a) Select the check box **Automatic Address Configuration (with DHCP)**.
   b) Select the **Accept IP Address of the Default Router** check box if you want this IP address to be used.
   c) Select the check box **Accept IP Address of the DNS Server** if required.
   d) Select the check box **Accept IP Address of the SNTP Server** if required.
7) If a fixed IP address is to be assigned to the WAN interface:
   a) Clear the check box **Automatic Address Configuration (with DHCP)**.
   b) Enter the desired **IP address** and **Netmask** of the WAN interface.
8) Enable the **NAT** check box.
9) If you also want to use Internet Telephony, select the item **Upload only** or **Upload and Download** as needed from the **Bandwidth Control for Voice Connections** drop-down list. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should only be activated for the upload direction to ensure that the download bandwidth reserved for voice transmission is not unnecessarily high.
10) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your Internet Service Provider.

11) Click on **OK & Next**, followed by **Finish**.

10.1.1.3 How to Configure Internet Access via an External Internet Router over the LAN with WAN Port Dedicated to ITSP

Prerequisites

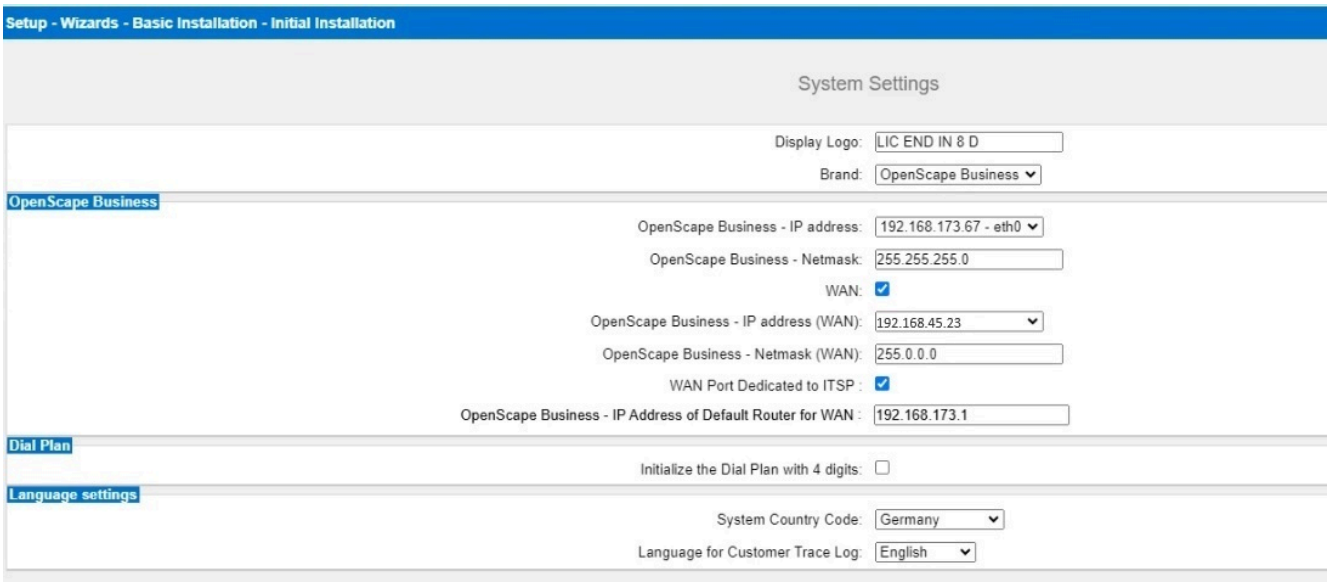
You have created a new network interface in the SLES.

You are in the **System Settings** window of the **Initial Installation** wizard.

Please note that this feature is only applicable for ITSPs that do not require the use of STUN in the provider settings.

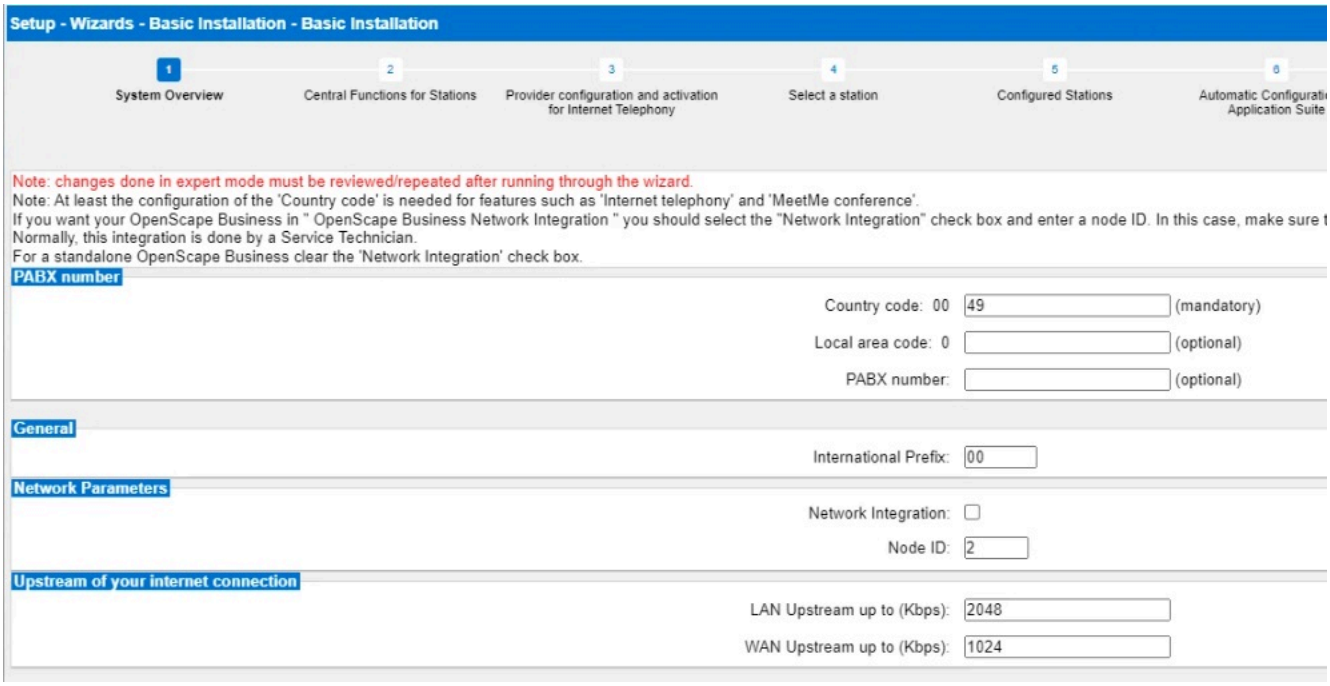
Step by Step

1) Enable the **WAN** check box and select the appropriate network interface. The option **WAN Interface Dedicated to ITSP** becomes available.
2) Click to enable the **WAN Interface Dedicated to ITSP** check box.



3) Click on **OK & Next**.
4) Navigate to **Setup > Basic Installation** and run the **Basic Installation** wizard.

5) Configure the maximum upstream values in the corresponding **LAN Upstream up to (Kbps)** and **WAN Upstream up to (Kbps)** fields.



6) Click on **OK & Next**.

7) After applying the configuration, a system restart is required.

NOTICE: STUN is not supported on the WAN interface when using the LAN/WAN feature. It is supported only on the LAN interface. If the ITSP requires STUN, SIP traffic must be routed through the LAN interface.

10.1.2 Internet Access via an Internet Modem

The **Internet Configuration** wizard helps you configure your Internet access via an Internet modem. An Internet modem is directly connected for this to the WAN port on your communication system. You can use an ISP that was preconfigured in the communication system or a standard ISP type (consult ISP for type).

To set up Internet access, you have the following options:

- **Setting up Internet Access via a Preconfigured ISP**

  You are using an ISP preconfigured in the communication system. You can then select your preconfigured ISP from a list.
- **Setting up Internet Access via the Standard ISP PPPoE**

  You are using the standard ISP type **Provider PPPoE**. Obtain the required settings from your ISP.
- **Setting up Internet Access via the Standard ISP PPTP**

  You are using the standard ISP type **Provider PPTP**. Obtain the required settings from your ISP.

Connection Clear-down Depending on the Tariff Model

Depending on the tariff model, you can define whether or not the connection to the ISP should be maintained in the event of inactivity.

- With the flat-rate tariff model, the Internet connection does not have to time out on inactivity. Many ISPs require forced timeout every 24 hours. You can enter the time when the connection should time out.
- With the time-based tariff model, the Internet connection should time out on inactivity. You can specify the inactivity timeout for connection clear-down (for instance, 60 seconds). The connection is automatically reestablished the next time an Internet request is made. If VPN is configured, the connection should not be cleared due to inactivity; the flat rate tariff model should hence be selected here.

NOTICE: Network-based programs or services can automatically set up an Internet connection and thereby incur additional connection charges for you if your tariff is time-based.

Bandwidth

Different bandwidths for downloading and uploading are usually provided by the ISP. The bandwidth is specified in Kbps. If Internet telephony is also used, the bandwidth is shared by voice and data transmission. We therefore recommend reserving sufficient bandwidth to guarantee good voice quality during voice transmission. However, this can lead to data transfer bottlenecks (for example, slower downloads) during periods with a high volume of voice transmissions.

You can choose whether bandwidth control for voice connections should be enabled only for uploading for both uploading and downloading. If the download bandwidth is high and the upload bandwidth is low, bandwidth control should be enabled only for uploading to prevent an unnecessarily high amount of download bandwidth from being reserved for voice transmissions.

NOTICE: About 128 Kbps of bandwidth is reserved for an Internet call.

10.1.2.1 How to Configure Internet Access via a Preconfigured ISP

You can use the **Internet Configuration** wizard to set up your Internet access via a preconfigured Internet Service Provider (ISP) in the communication system.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Your ISP's Internet access data is available (for example, user account, password, etc.).

Step by Step

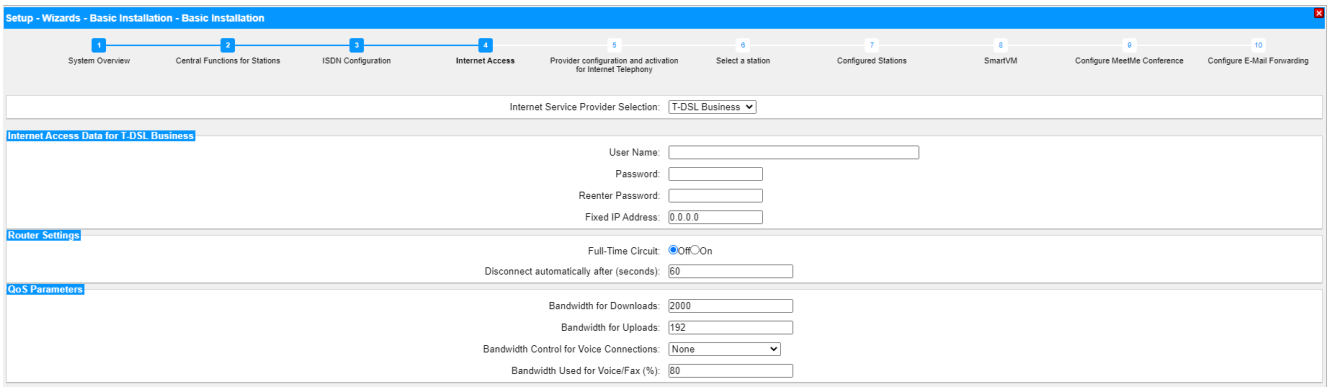
1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Network / Internet**.

3) Click **Edit** to start the **Internet Configuration** wizard.

4) Disable the **No Internet Access** check box.

5) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.



6) Select your ISP from the **Internet Service Provider Selection** drop-down list.

7) Enter the access data that you received from your ISP in the **Internet Access Data for...** area. The fields in this area ate provider-specific. When entering your data, bear in mind that the input is case-sensitive!

8) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:

   - If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be deactivated (e.g., 04:59).
   - If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

9) Set the following values in the **QoS Parameters** area:

   a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

   b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

10) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

11) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).

   a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).

   b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition,

customer-specific parameters (shown in *italics* in the example) must be supplemented.

```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```

c) Enter the **User name** and the **Password** of your DynDNS account.
d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.
e) Test the DynDNS account with **Connection test**.
f) After the test succeeds, click **OK**.
g) Click **OK & Next**.

12) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

13) Click **Finish**. The communication system performs a restart.

10.1.2.2 How to Configure Internet Access via a Standard ISP PPPoE

You can use the **Internet Configuration** wizard to set up your Internet access via the standard Internet Service Provider PPPoE.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		

Field	Description	Value from ISP
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Network / Internet**.

3) Click **Edit** to start the **Internet Configuration** wizard.

4) Disable the **No Internet Access** check box.

5) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.

6) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPPoE**.

7) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP Address Negotiation** drop-down list, select the item **Use configured IP address**.

8) Depending on your tariff model, select one of the following two options under **Full-Time Circuit** in the **Router Settings** area:

- If you have a flat rate tariff model, enable the radio button **On**. In the **Forced Disconnect at (hour:min)** field, enter the time at which the Internet connection is to be deactivated (e.g., 04:59).
- If you have a time-based tariff model, enable the radio button **Off**. In the **Disconnect automatically after (seconds)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

9) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.

- Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. The customary standard is the **CHAP Client** authentication mode.
- Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.

10) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.

11) Set the following values in the **QoS Parameters of Interface** area:

a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

12) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.
13) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).
    a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).
    b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

       `http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
    c) Enter the **User name** and the **Password** of your DynDNS account.
    d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.
    e) Test the DynDNS account with **Connection test**.
    f) After the test succeeds, click **OK**.
    g) Click **OK & Next**.
14) If you have a static public IP address or do not want to use a VPN or remote access, click **No DynDNS**.
15) Click **Finish**.

10.1.2.3 How to Configure Internet Access via a Standard ISP PPTP

You can use the **Internet Configuration** wizard to set up your Internet access via the standard Internet Service Provider PPTP.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The following ISP-specific Internet access data is available to you:

Field	Description	Value from ISP
IP Parameters (only for a fixed IP address)		
Remote IP Address of the PPP Connection	IP address of your ISP's server.	
Local IP Address of the PPP Connection	IP address that was assigned to you by your ISP for Internet access.	
PPTP Parameter		
Local IP Address of the Control Connection	IP address that was assigned to you by your ISP for the PPTP connection. The default value is 10.0.0.140.	

Field	Description	Value from ISP
Remote IP Address of the Control Connection	IP address of your ISP's server for the PPTP connection. The default value is 10.0.0.138.	
Remote Netmask for the Control Connection	Subnet mask that was assigned to you by your ISP for the PPTP connection. The default value is 255.255.255.248.	
Authentication (via PAP or CHAP). PAP is seldom used, since the authentication is unencrypted.		
PPP User Name	User name that was assigned to you by your ISP for the PPP connection.	
PAP Authentication Mode	Authentication mode for the PPP connection over PAP: **PAP Client**, **PAP Host** or **Not used**.	
PAP Password	Password assigned to you by the ISP for PAP authentication	
CHAP Authentication Mode	Authentication mode for PPP connection via CHAP: **CHAP Client**, **CHAP Host**, **CHAP Client and Host** or **Not used**.	
CHAP Password	Password assigned to you by the ISP for CHAP authentication	
QoS Parameters of Interface		
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.	
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.	

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click **Edit** to start the **Internet Configuration** wizard.
4) Disable the **No Internet Access** check box.
5) Activate the radio button **DSL at WAN Port directly** and click **OK & Next**.
6) From the **Internet Service Provider Selection** drop-down list, select the standard ISP Type **Provider PPTP**.
7) The **IP parameters** check box in the **IP Parameters** area should only be enabled if the ISP requires an adjustment of these parameters. In this case, enter the values that you have received from your ISP in the **Remote IP Address of the PPP Connection**, **Local IP Address of the PPP Connection** and **Max. Data Packet Size (bytes)** fields. From the **IP Address Negotiation** drop-down list, select the item **Use configured IP address**.
8) Enter the values that you received from your ISP in the **PPTP Parameter** area.

9) If you have a time-based tariff model, select the **Short Hold** check box. In the **Short Hold Time (sec)** field, enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds).

10) The settings in the **Authentication** area depend on whether or not the ISP requires authentication via PPP.

- Authentication required by ISP: Make sure that the check box **PPP Authentication** is enabled. Enter the Internet access name of the ISP as the PPP user name. Make the PAP and CHAP settings, as assigned to you by your ISP.
- Authentication not required by ISP: Make sure that the check box PPP Authentication is disabled.

11) If you want to use NAT, enable the **NAT** check box (enabled by default) in the **Address Translation** area.

12) Set the following values in the **QoS Parameters of Interface** area:

a) In the **Bandwidth for Downloads** and **Bandwidth for Uploads** fields, enter the bandwidth in Kbps for downloads and uploads, respectively, as provided by your ISP.

b) If you want to use Internet Telephony as well, open the drop-down list **Bandwidth Control for Voice Connections** and select the item **Upload only** or **Upload and Download**, as required. In the field **Bandwidth Used for Voice/Fax (%)**, enter how much bandwidth is to be reserved for voice and fax connections as a percentage value (default value: 80%).

13) Click **OK & Next**. You are taken to the **Configure DynDNS-Account** window.

14) If you want to use a VPN or remote access and do not have a public static IP address, you will need to have already applied for and set up a DynDNS account (at dyndns.org, for example).

a) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).

b) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

`http://www.anydns.info/update.php?`
`user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Enter the **User name** and the **Password** of your DynDNS account.

d) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.

e) Test the DynDNS account with **Connection test**.

f) After the test succeeds, click **OK**.

g) Click **OK & Next**.

15) If you have a public static IP address or do not want to use a VPN or remote access, click **No DynDNS**.

16) Click **Finish**. The communication system performs a restart.

10.1.3 WAN port

WANs (**W**ide **A**rea **N**etwork) are used to network different LANs (**L**ocal **A**rea **N**etwork) as well as individual PCs with one another. An Internet modem for access to the Internet can be connected to the WAN port.

The WAN port must not be used for the networking of network nodes and for connecting IP stations or IP clients.

10.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) is an Internet service that assigns a fixed DNS name to an IP address that changes dynamically.

OpenScape Business X makes the DynDNS service available if an Internet modem is connected to the WAN port of OpenScape Business X and the communication system is used as an Internet router. If this is not the case, DynDNS is set up in the external Internet router in the infrastructure of the customer.

DNS Name

With DynDNS, a client who is connected to the Internet with a dynamic IP address can always be addressed with the same name, the DNS name.
A DynDNS account with a DynDNS provider (such as www.dyndns.org) is needed for this. If the communication system is assigned a new IP address (for example, by the Internet Service Provider), this IP address is automatically sent to the DynDNS provider and saved in the DynDNS account. The refresh interval is adjustable. If a DNS name is addressed, a request is sent to the DynDNS provider to translate the name into the IP address currently valid. The entire DNS name (also known as the domain name) is composed of a host name of your choice (myhost, for instance) and the selected DynDNS provider (dyndns.org, for instance), producing, in this instance, myhost.dyndns.org. More information on this can, for example, be found at the Internet address:

`http://www.dyndns.org/services/dyndns`

DynDNS also lets you set up a virtual private network (VPN) over an Internet Service Provider that supplies dynamic IP addresses. This enables teleworkers, for example, to access the internal network via the Internet. More Information can be found under Virtual Private Network (VPN) .

Mail Exchanger

The Mail Exchange entry (MX record) in the Domain Name Service (DNS) specifies the IP address to which e-mails should be sent for the domain name configured (myhost.dyndns.org, for instance). The mail server (Mail Exchanger) must be located at the IP address specified. An e-mail address for this domain name could be as follows: mymail@myhost.dyndns.org.

The Backup MX function buffers e-mails that could not be delivered to the Mail Exchanger specified above (because of temporary unavailability, for instance) and delivers them as soon as Mail Exchanger availability is restored.

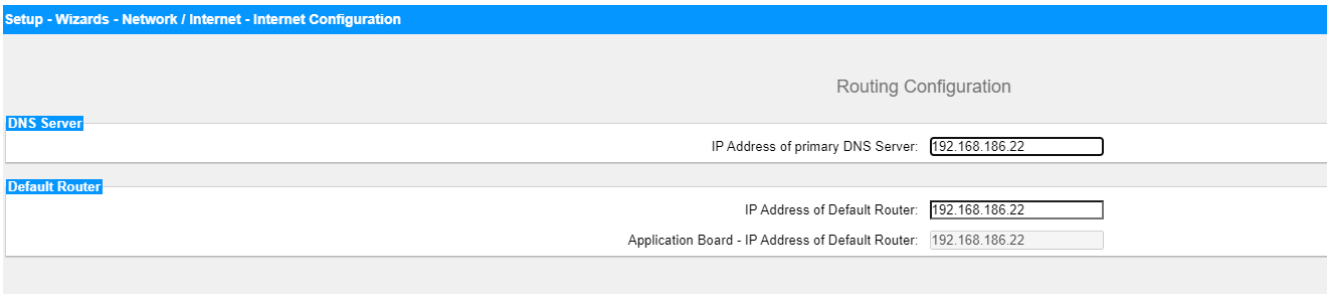
10.1.4.1 How to Configure the DynDNS Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

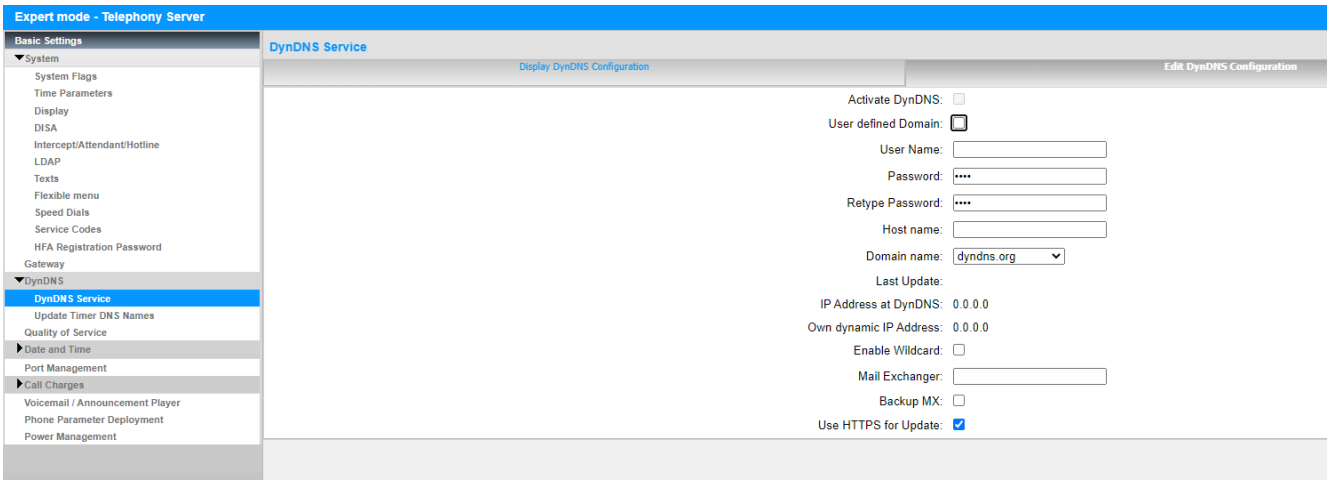
Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) Click on **DynDNS** in the menu tree.
4) Click **Update Timer for DNS Names**.



5) Activate the radio button **Update DNS Names**.
6) This timer value applies only to VPN: in the **Update Timer value for DNS Names** field, enter the time interval (in seconds) after which the VPN component checks whether any DNS names in the VPN configuration are resolved into new IP addresses (VPN with dynamic IP addresses). If this is the case, the VPN will be reconfigured with the new IP addresses.

   The default value for this field is `180`, which corresponds to an update interval of 3 minutes.
7) In the menu tree, click on **DynDNS Service**.
8) Click the **Edit DynDNS Configuration** tab.



9) Select the **Activate DynDNS** check box.
10) If your desired DynDNS provider is included in the **Domain name** drop-down list, select it from that list (e.g., dyndns.org).
11) If your desired DynDNS provider is not included in the **Domain name** drop-down list, select the **User defined Domain** check box. Enter the desired DynDNS provider in the **Domain name** field and enter the update URL

of the DynDNS provider in the **Update URL** field. The structure of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.

`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`

Example of an update URL with base64-encoded authentication:

`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx`

<b64>...</b64> for Base64-encoded parameters

12) Enter the user name for your DynDNS account with the DynDNS provider in the **Login Name** field.

13) Enter the password of your DynDNS account with the DynDNS provider in the **Password** and **Retype Password** fields.

14) Enter the host name assigned to you by the DynDNS provider, omitting the domain name, for instance, myhost, in the **Hostname** field. Your complete domain name would then be myhost.dyndns.org, for example.

15) Only visible for DynDNS providers included in the **Domain name** drop-down list: Activate the radio button **Enable Wildcard** if you want queries to a subordinate domain name such as any.myhost.dyndns.org to also be accepted.

16) Only visible for DynDNS providers included in the **Domain name** drop-down list: Activate the radio button **Use HTTPS for Update** if you want to use a secure connection to the DynDNS provider to update the IP address.

17) Click **Apply**, followed by **OK**.

10.1.4.2 How to Define the Mail Exchanger

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

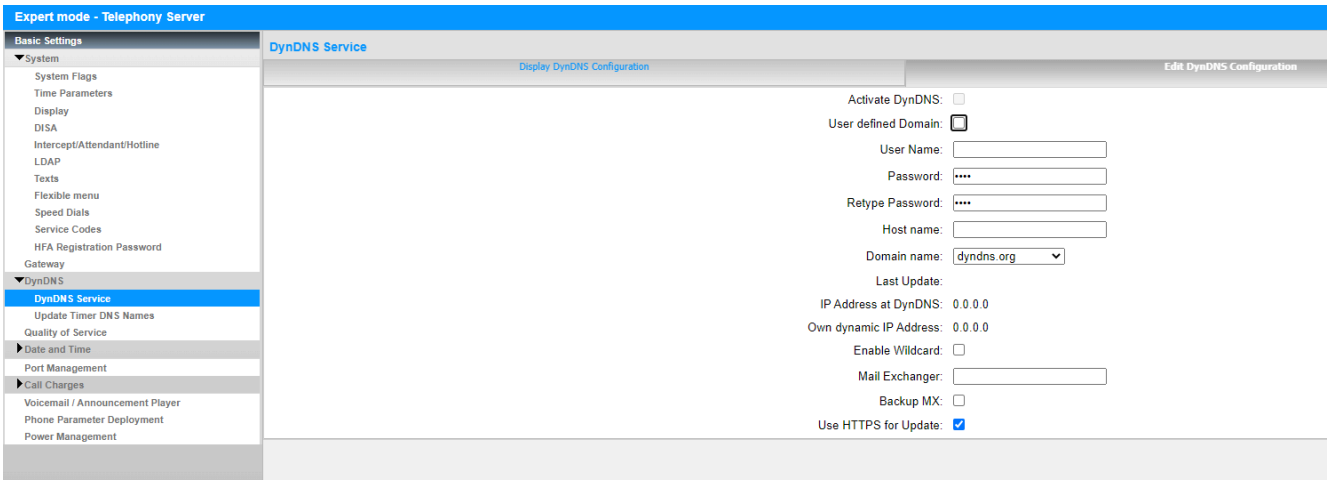
1) In the navigation bar, click on **Expert Mode**.

2) Click **Telephony** > **Basic Settings** in the navigation tree.

3) Click on **DynDNS** in the menu tree.

4) Click on **DynDNS Service**.

5) Click on the **Edit DynDNS Configuration** tab.



6) Enter the IP address of the mail server (Mail Exchange entry or MX record) in the **Mail Exchanger** field.
7) If necessary, activate the **Backup MX** radio button.
8) Click on **Apply**, followed by **OK**.

10.2 CO Access via ITSP

In order to make calls over the Internet, you will need access to an Internet Telephony Service Provider (ITSP, SIP Provider). To do this, an Internet telephony connection and a user account must be applied for from the ITSP.

Connection to the ITSP

The communication system uses the options described in the section on "Internet Access" to reach the ITSP (OpenScape Business X: via LAN or WAN / OpenScape Business S: exclusively via LAN).

The ITSP access based on SIP (Session Initiation Protocol) for signaling and RTP (Realtime Transport Protocol) for voice and data.

Internet Telephony Service Providers do not always offer the same range of SIP features. Consequently, only ITSPs certified for the communication system should be used. A list of certified ITSPs as well as the certification process can be found at the following link:

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

NOTICE: Special numbers and emergency numbers, which are not supported by the ITSP, should be routed over fixed network connections.

In the event of ITSP failure, fixed network connections via least cost routing (LCR) can be used as a fallback solution.

ITSP user account

The ITSP user account (SIP User Account) must be applied for from the ITSP. The ITSP provides a SIP Registrar server at which the communication system must first log in (provider-specific) for this purpose.

NOTICE: A registration is not necessary if static IP authentication or a VPN tunnel is used by the ITSP.

Mobile Extension (MEX)

This feature is offered by some mobile phone operators in connection with the MDA (mobile direct access) service. It enables mobile phones/smartphones to be integrated as internal subscribers in a communication system.

This feature can only be used only with an Internet telephony DID connection. To do this, the MEX number provided by the ITSP must be entered when configuring the ITSP. At the ITSP, the call number of the mobile phone is associated with the MEX number. In addition, the mobile phone or smartphone must be configured in the communication system as a Mobility station (see Configuring myPortal to go and Mobility Entry).

Short Description:

- The mobile phone operator offers a flat-rate for the mobile phone.
- One Number Service: the mobile phone can be reached under a single fixed network number, which is also communicated to the other party.
- The presence status and connection status of mobile phones are visible exactly as for normal internal subscribers.
- Every phone call from or to the mobile phone is performed exclusively via OpenScape Business in combination with a certified ITSP.
- The mobile phone number of the mobile phone is not known to the outside, i.e., the mobile phone cannot be called directly. It can also not make any direct outbound calls. All calls are conducted through OpenScape Business.
- The mobile phone can be integrated into system-internal teams.
- UC applications such as myPortal for Desktop and myPortal for Outlook can be used in the same way as for internal subscribers.
- myPortal to go is available on the road.
- Embedded mobile phones identify themselves by name when calling an internal subscriber.
- The digit analysis and call routing in the system or network occurs as for any other internal station (e.g., allowed numbers, denied numbers, LCR rules)
- The ITSP uses special call signaling from/to the OpenScape Business, which must be administered accordingly.
- Every integrated mobile phone requires a Mobility User license.
- To use UC applications, a UC Client license is additionally required.

10.2.1 Configuring an ITSP

It is possible to configure predefined and new Internet Telephony Service Providers (ITSPs). You can configure one or several accounts for each ITSP. Up to 8 ITSPs may be active simultaneously.

Additional information on ITSPs and their features can be found here:

http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview

NOTICE: Configuration examples can be found on the Internet at the **Unify Experts Wiki** under *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

Assigning the ITSP Phone Numbers

- In the case of an **Internet Telephony Station Connection**, the ITSP provides individual numbers such as 70005555, 70005556, etc. These individual call numbers are then assigned manually as the internal call numbers of the subscribers.
- In the case of an **Internet telephony point-to-point connection**, the ITSP provides a call number range, e.g., (+49) 89 7007-100 to (+49) 89 7007-147. The call numbers from the range are then assigned manually as the internal call numbers of the subscribers.

These two connection types can be combined as appropriate.

Alternatively, the ITSP phone numbers can be entered as the DID call numbers of the subscriber for both connection types during the station configuration.

Internal call number	Name	DID
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

The ITSP call numbers thus result from the configured PABX number (e.g., country code 49) and the entered DID numbers in long format. This has advantages for the digit analysis and call management, even in an internetwork. The ITSP connection is thus DID-enabled for another node, for example.

A further CO trunk connection via ISDN is only possible to a limited extent in this case.

Multisite Management

The subscribers of the communication system can be assigned to different sites (with different area codes, for example). Each site is assigned a route, and each route is assigned an ITSP registration. A maximum of 8 ITSP registrations can be managed. One registration per ITSP is possible or even multiple registrations at one ITSP. Each ITSP registration can be assigned an area code, and multiple subscribers can then be assigned to it. The connection between the subscribers at the different sites and the communication system occurs via a VPN. All sites must be located within one country and use the same CO access code (see also *Networking OpenScape Business in Hosting Environments*, Scenario 1b).

Using ITSP Templates

The default is to use a preconfigured ITSP template. To do this, the own access data and phone numbers are entered in the template, and this is then activated.

In Expert mode, you can also edit a preconfigured ITSP template and save it as a new template.

Updating ITSP Templates

The preconfigured ITSP templates are automatically updated after a software update of the system if there are new preconfigured ITSP templates in that update or more recent default values for existing preconfigured templates.

If the ITSP of a template is already activated, the update is not done automatically, since important changes could otherwise be overwritten when updating the default values. Consequently, the update can be performed manually in the Expert mode if required. The default values will then need to be customized again to suit individual requirements.

Line Direction Mode

Individual lines of an ITSP trunk can be blocked for outgoing and/or incoming traffic. The following line direction modes are possible:

- outgoing only
- incoming only
- outgoing and incoming (default)

The line direction is evaluated when the communication system must reserve an ITSP line for an incoming or outgoing call.

10.2.1.1 How to Configure a Predefined ITSP

The **Internet Telephony** wizard can be used to configure and activate a predefined Internet Telephony Service Provider (ITSP). You can configure one or several accounts for each ITSP.

Prerequisites

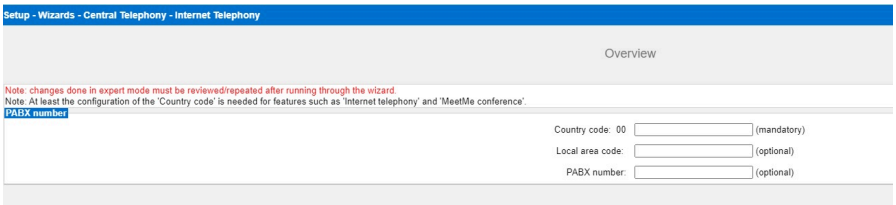
The Internet connection is operational.

Your ITSP's Internet telephony access data is available (for example, user account, password and Internet telephony number).

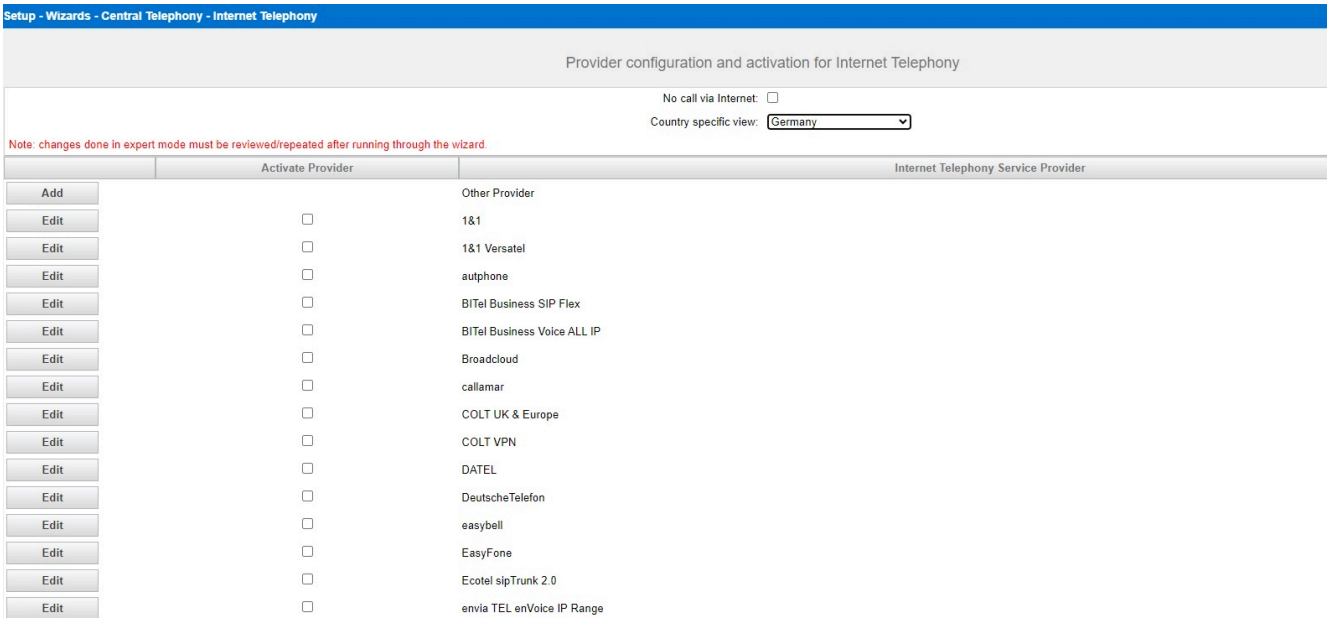
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click **Edit** to start the **Internet Telephony** wizard.



4) Clear the **No call via Internet** check box. A country-specific list of the possible ITSPs is displayed. The list contains the predefined ITSPs for the selected country and ITSPs you have created.



5) If you want to change the preset country, select the desired country from the **Country specific view** drop-down list to display the ITSPs that are available for this country.

6) If required, click **Display Status** to check which ITSPs have already been activated and which Internet telephony subscribers have already been configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.

7) To configure the predefined ITSP, click **Edit** in the line associated with the desired ITSP.

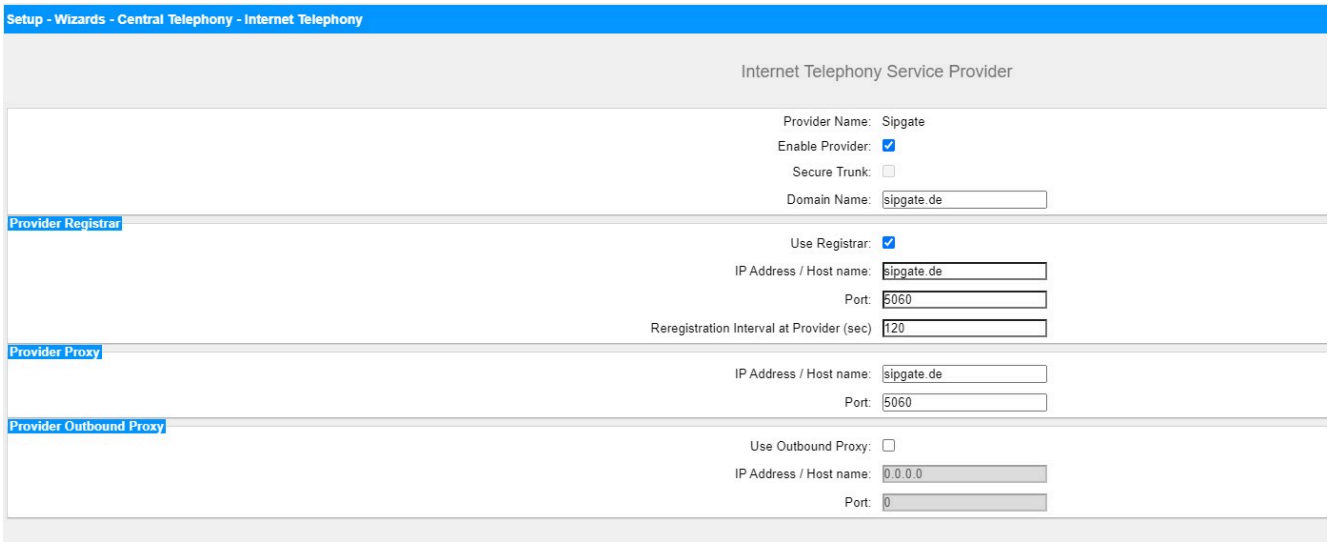
8) Activate the check box **Enable Provider**.

9) If the provider supports secure connection, the check box **Secure Trunk** can be activated.

10) The values for "**Provider Registrar**", "**Provider Proxy**", "**Provider Outbound Proxy**" and "**Provider Feature**" (if enabled) are predefined according to the needs of most ITSPs. For some ITSPs customer specific server addresses are used. In such a case the fields which are not greyed out needs to be filled according to the documentation received from the ITSP.

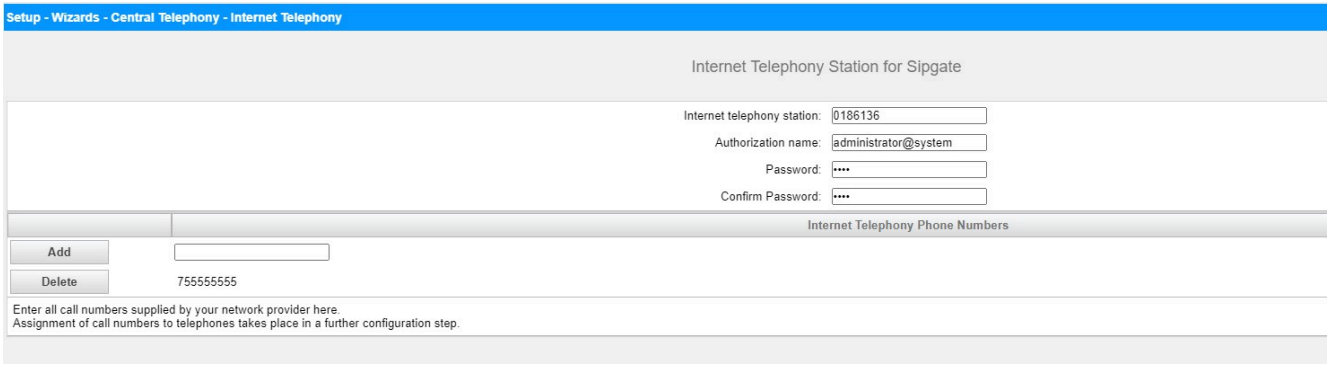
11) If the provider supports Call deflection the section Provider Feature is shown and you can activate the call deflection feature. When Call

deflection is activated call forwarding is performed in the provider network, call management in the system is not effective.



12) Click **OK & Next**.

13) Click **Add** to configure your ITSP accounts with the corresponding Internet telephony numbers. The fields that will then be displayed are provider-specific.



14) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

More details can be found at http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

15) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

NOTICE: If no registration is used, **Authorization name** is grayed out and cannot be configured.

---

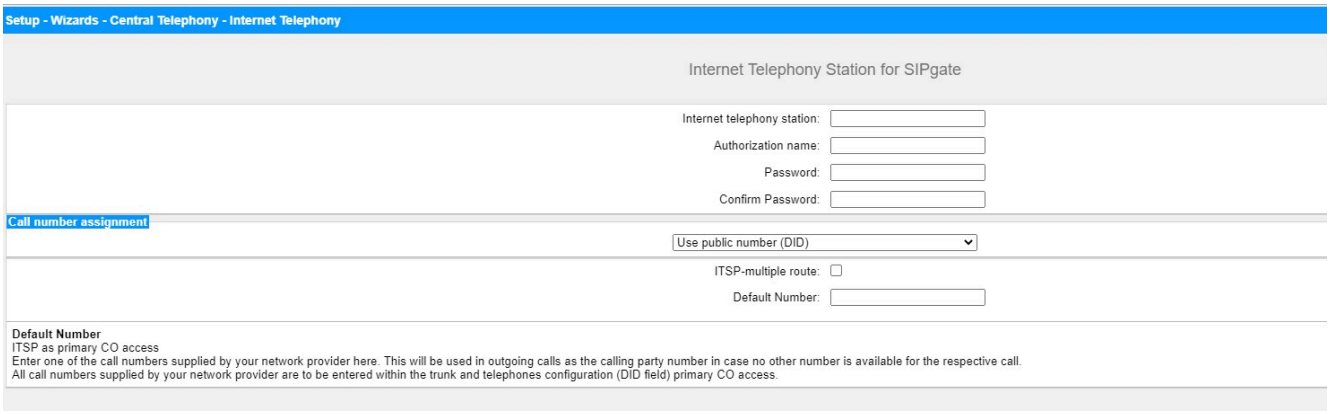
16) Enter the password you received from the ITSP in the **New Password** and **Confirm Password** fields. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

NOTICE: If no registration is used, **Password** is grayed out and cannot be configured.

---

17) Assignment of Internet telephony phone numbers - Option 1:

Use public number (DID): the Internet telephony phone numbers (DID) of your Internet telephony connection are configured in the stations setup (in the **DID** fields). No mapping configuration during the ITSP configuration is necessary.

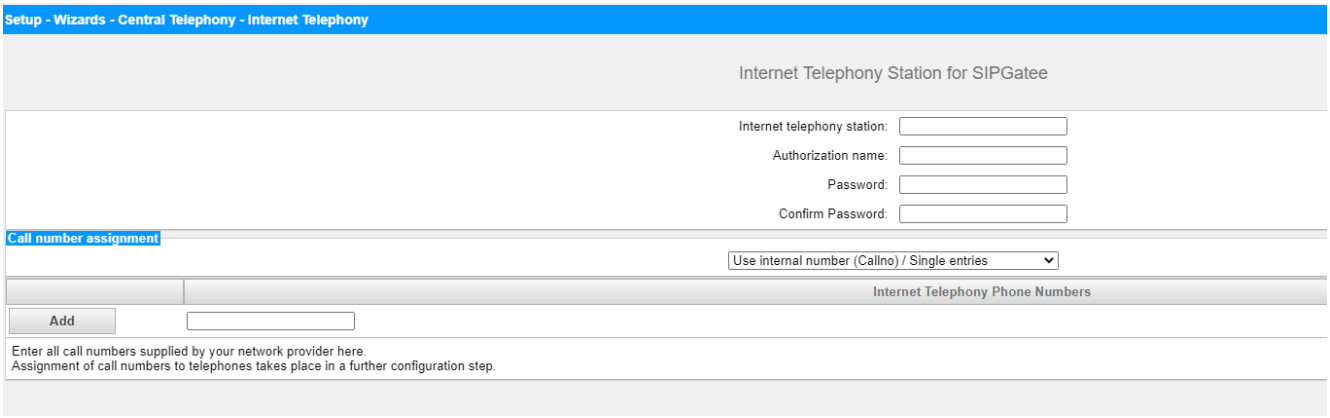


a) Select the option field **Use public number (DID)** in the **Call number assignment** area.
b) Under **Default Number**, enter the phone number to be used for outgoing calls when no caller DID number is available.
c) If your ITSP supports the "Mobile Extension (MEX)" feature, enter the MEX number provided by the ITSP (8 positions, digits only) under **MEX Number**. If your ITSP does not support the "Mobile Extension (MEX)" feature, the **MEX Number** field is not displayed.
d) If multiple routes need to be configured, activate the check box **ITSP-multiple route**.
e) Enter the **ITSP route prefixes** assigned to the route and click on **Add**.

18) Assignment of Internet telephony phone numbers - Option 2:

Use internal number (CalIno) / Single entries: You have an ITSP which needs SIP registration for each call number (e.g. 70005555, 70005556,...). For each call number an Internet Telephony Station must be created and a

single call number needs to be assigned. If your ITSP allows multiple call numbers with one registration Option 1 should be used.



a) Select the option field **Use internal number (CalIno) / Single entries** in the **Call number assignment** area.

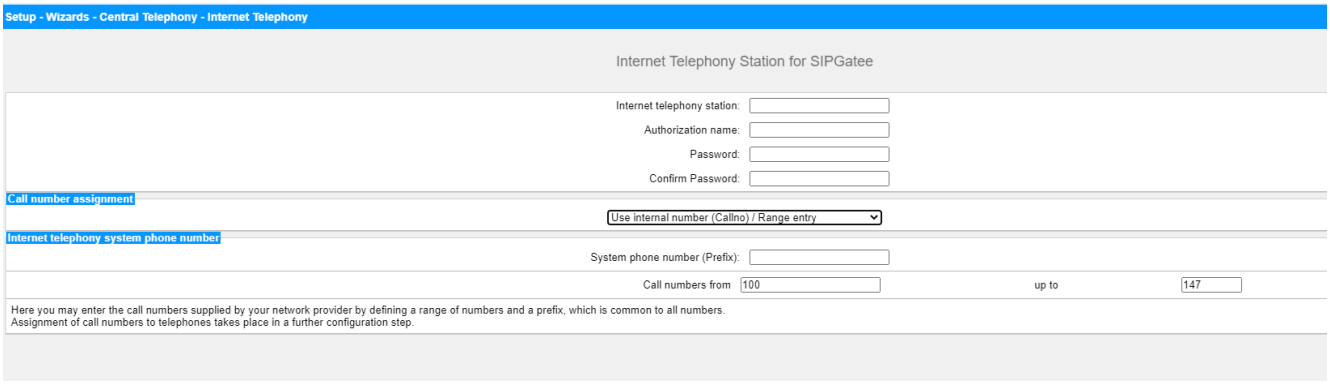
b) In the **Internet Telephony Phone Numbers** area, enter one of the Internet telephony phone numbers provided by the ITSP in the field next to the **Add** button and then click **Add**.

c) To assign further Internet telephony numbers to the account, repeat step b).

19) Assignment of Internet telephony phone numbers - Option 3:

Use internal number (CalIno) / Range entry: the use of this option is deprecated, for DID configuration option 1 should be used.

You have an Internet telephony point-to-point connection and have received a call number range as Internet telephony phone numbers (e.g., +49) 89 7007-100 to (+49) 89 7007-147. You then assign the call numbers from the call number range as the internal call numbers of the subscribers.



a) Select the option field **Use internal number (CalIno) / Range entry** in the **Call number assignment** area.

b) Enter the system phone number under **System phone number (prefix)**.

c) Enter the desired DID number range for the Internet telephony station in the 'from' **and** 'to **' fields after** Direct inward dialing band. The range entered by default is 100 - 147.

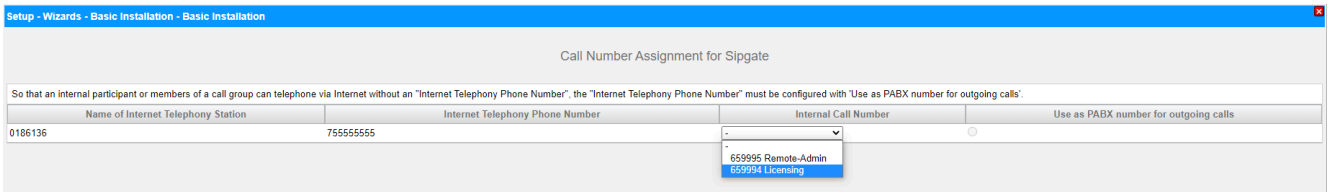
20) Click **OK & Next**.

21) If you want to configure additional accounts, repeat steps 13 through 20.

22) Click **OK & Next**. You will see an overview of which Internet telephony phone numbers are assigned to accounts.

23) Assign one internal station number each to every Internet telephony phone number.

This step is not required if you have selected option 1 for the assignment of the Internet telephony phone numbers. In this case, the assignment is made when the configuring the stations (i.e., the telephones and subscribers) in the **DID** field. The screen is also visible in this case but not editable.



a) To do this, select an internal call number in the appropriate line from the **Internal Call Number** drop-down list.

b) If subscribers without Internet telephony phone numbers or members of a call group are to be allowed to make external calls via the Internet, the radio button **Use as PABX number for outgoing calls** must be activated. The radio button can be activated for only one single Internet telephony phone number.

24) Click **OK & Next**. You will again see an overview of the possible ITSPs here. The enabled ITSPs are identified with a check mark in the **Enable Provider** column. With Display Status you can check the connection status. If you are having connection problems with an already activated ITSP, you can register it again with **Restart ITSP** on this page.

25) Click **OK & Next**.

26) Enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field. Please do not confuse this with the download speed!

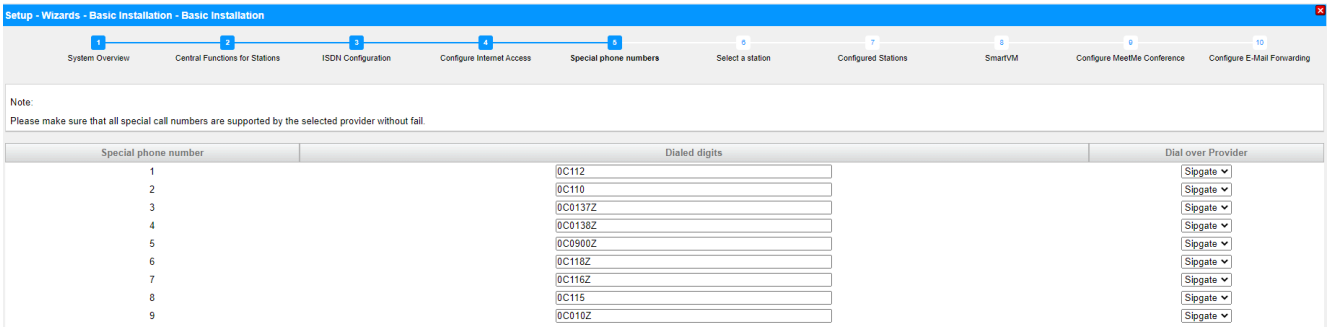
NOTICE: The number of simultaneous Internet calls permitted is displayed in the **Number of Simultaneous Internet calls** field. If the voice quality deteriorates due to the network load, you will need to reduce the number.

For more information about the number of simultaneous Internet calls, please refer to Limiting the Number of Simultaneous Calls via an ITSP on page 781.

---

27) Click **OK & Next**.

28) Enter the special numbers you want in the **Dialed digits** column.



The following station number entries are valid:

- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

29) Use the **Dial over Provider** column to specify whether the special number should be dialed via ISDN or an ITSP. Only the active ITSP is displayed.

NOTICE: Ensure that emergency numbers can always be dialed. If you want to dial emergency numbers via an Internet Telephony Service Provider, you must make sure that the ITSP supports this feature.

---

30) Click **OK & Next**. The status of your ITSP will be displayed.

31) Click **Next** followed by **Finish**. Following this step, please run the **CO Trunk ISDN / Analog / ITSP** wizard to set the prioritization for the exchange line seizure (for example: Exchange Line Seizure First over ITSP and Next over ISDN).

10.2.1.2 How to Add a New ITSP

The **Internet Telephony** wizard can be used to configure and activate a new Internet Telephony Service Provider (ITSP). You can configure one or several accounts for each ITSP.

Prerequisites

The Internet connection is operational.

You are logged on to the WBM with the **Advanced** profile.

The following ITSP-specific Internet access data is available:

Field	Description	Value from ISP
Gateway Domain Name	Gateway Domain Name of the ITSP Usually identical to the host name (e.g., sip-voice.de)	
Provider Registrar		

Field	Description	Value from ISP
Use Registrar	Predefined by the ITSP and generally always set (not required for ITSPs which use static IP authentication).	
IP address/Host name	Host name or IP address of the Registrar server (e.g., sip-voice.de).	
Port	Port number of the Registrar server (e.g., 5060).	
Reregistration Interval at Provider (sec)	Interval (in seconds) at which ITSP registration is repeated. The value of the interval must not be 0 and must not be set too high because on repeating the registration at the ITSP, a dropped connection can also be detected, and an alternate route (via ISDN or an alternate Provider) may be selected if required. Default value: 120 seconds.	
Provider Proxy		
IP address/Host name	Host name or IP address of the proxy server (e.g., sip-voice.de). This is usually identical with the Provider Registrar entry.	
Port	Port number of the proxy server (e.g., 5060). This is usually identical with the Provider Registrar port number.	
Provider Feature		
Call deflection	Visible only if the selected Base template support Call deflection	
Provider Outbound Proxy		
Use Outbound Proxy	Only set if the ITSP uses an outbound proxy.	
IP address/Host name	Host name or IP address of the outbound proxy	
Port	Port number of the outbound proxy	
Provider Inbound Proxy		
Use Inbound Proxy	Only set if the ITSP uses a second proxy.	
IP address/Host name	Host name or IP address of the second proxy	
Port	Port number of the second proxy	
Provider STUN		
Use STUN	Used only if STUN functionality is required. Also enables global STUN mode.	

Field	Description	Value from ISP
IP address/Host name	STUN IP address if the ITSP is using a STUN server.	
Port	STUN port number if the ITSP is using a STUN server.	

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click **Edit** to start the **Internet Telephony** wizard.
4) Clear the **No call via Internet** check box. A country-specific list of the possible ITSPs is displayed. The list contains the predefined ITSPs for the selected country and any already created ITSPs.
5) If required, click **Display Status** to check which ITSPs have already been activated and which Internet telephony subscribers have already been configured under each ITSP. You can activate a maximum of 8 ITSPs. Click **OK** when finished.
6) Click **Add** to set up a new ITSP. A configuration window for the new ITSP appears.
7) Select a **Base Template** from the drop-down list. This option makes possible to have the same ITSP configured in several routes.
8) Assign a name of your choice for the ITSP in the **Provider Name** field.

NOTICE: The maximum limit of characters is 10.

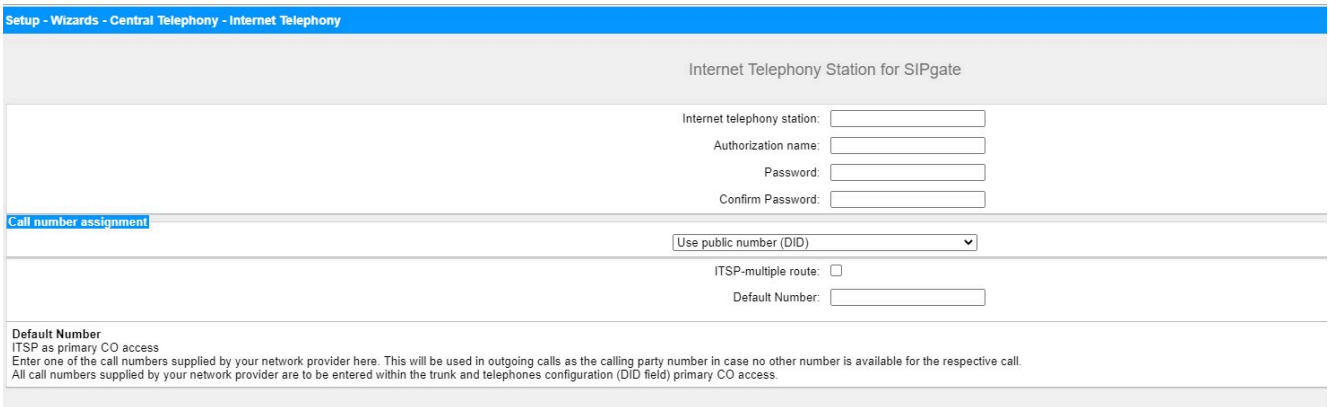
---

9) Activate the check box **Enable Provider**.
10) Enter the values provided by your ITSP in the remaining areas (see table immediately after prerequisites).

NOTICE: The values under the "Extended SIP Provider Data" may only be changed by authorized service personnel, in collaboration with Development!

---

11) Click **OK & Next**.
12) Click **Add** to configure your ITSP accounts with the corresponding Internet telephony numbers. The fields that will then be displayed are provider-specific.



13) Enter the credentials for your account in the **Internet Telephony Station** field. You received this data from your ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc.

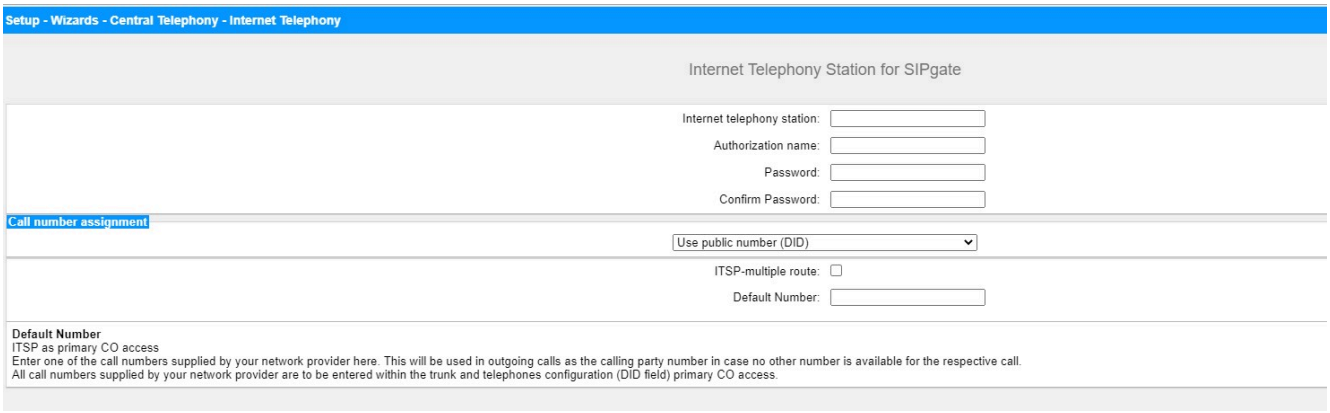
    More details can be found at http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers

14) Enter the authorization name in the **Authorization name** field. You received this data from your ITSP. If you have not received any authorization name, enter the same data you entered under **Internet Telephony Station**.

15) Enter the password you received from the ITSP in the **New Password** and **Confirm Password** fields. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

16) Assignment of Internet telephony phone numbers - Option 1:

    Use public number (DID): the Internet telephony phone numbers (DID) of your Internet telephony connection are configured in the stations setup (in the **DID** fields). No mapping configuration during the ITSP configuration is necessary.



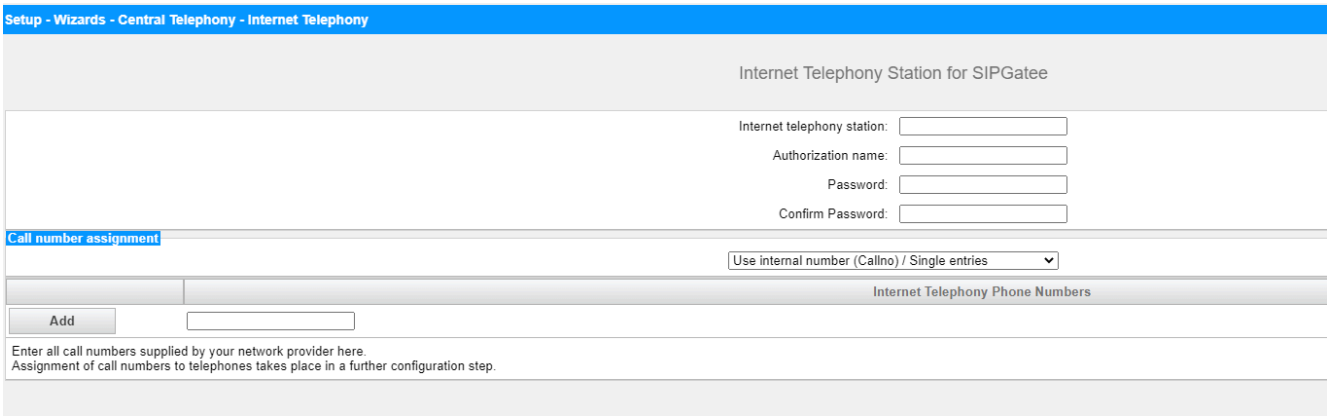
    a) Select the option field **Use public number (DID)** in the **Call number assignment** area.
    b) Under **Default Number**, enter the phone number to be used for outgoing calls when no caller DID number is available.
    c) If your ITSP supports the "Mobile Extension (MEX)" feature, enter the MEX number provided by the ITSP (8 positions, digits only) under **MEX Number**.
    d) Activate the check box **ITSP-multiple route**.
    e) Enter the **ITSP route prefixes** assigned to the route and click on **Add**.

    NOTICE: In order to configure multiple routes the above steps have to be repeated. More information can be found in the Unify wiki at: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#General_Configuration_guides

17) Assignment of Internet telephony phone numbers - Option 2:

    Use internal number (CalIno) / Single entries: You have an ITSP which needs SIP registration for each call number (e.g. 70005555, 70005556,...). For each call number an Internet Telephony Station must be created and a

single call number needs to be assigned. If your ITSP allows multiple call numbers with one registration Option 1 should be used.



a) Select the option field **Use internal number (CalIno) / Single entries** in the **Call number assignment** area.

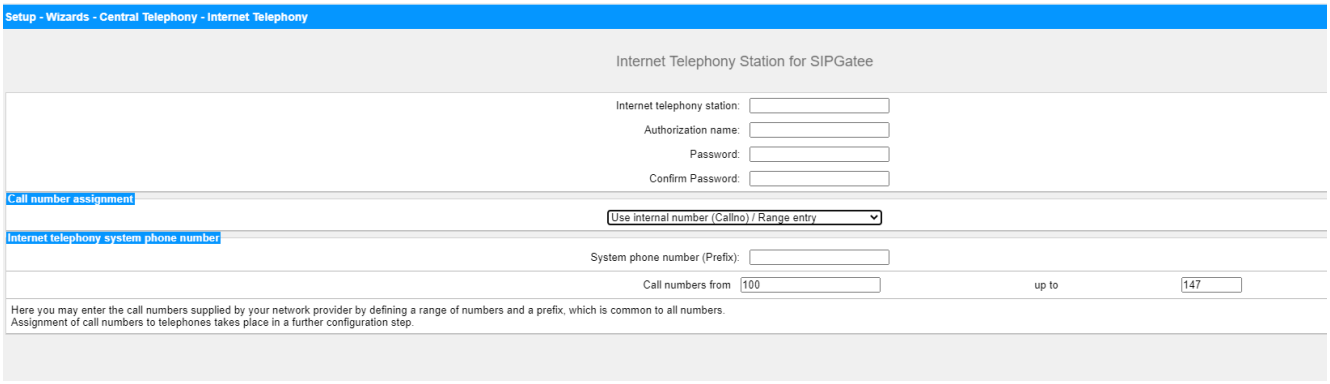
b) In the **Internet Telephony Phone Numbers** area, enter one of the Internet telephony phone numbers provided by the ITSP in the field next to the **Add** button and then click **Add**.

c) To assign further Internet telephony numbers to the account, repeat step b).

18) Assignment of Internet telephony phone numbers - Option 3:

Use internal number (CalIno) / Range entry: the use of this option is deprecated, for DID configuration option 1 should be used.

You have an Internet telephony point-to-point connection and have received a call number range as Internet telephony phone numbers (e.g., +49) 89 7007-100 to (+49) 89 7007-147. You then assign the call numbers from the call number range as the internal call numbers of the subscribers.



a) Select the option field **Use internal number (CalIno) / Range entry** in the **Call number assignment** area.

b) Enter the system phone number under **System phone number (prefix)**.

c) Enter the desired DID number range for the Internet telephony station in the 'from' **and** 'to **' fields after** Direct inward dialing band. The range entered by default is 100 - 147.

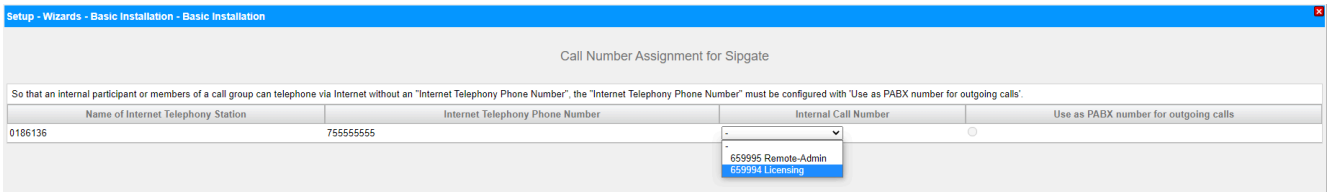
19) Click **OK & Next**.

20) If you want to configure additional accounts, repeat steps 12 through 19.

21) Click **OK & Next**. You will see an overview of which Internet telephony phone numbers are assigned to accounts.

22) Assign one internal station number each to every Internet telephony phone number.

This step is not required if you have selected option 1 for the assignment of the Internet telephony phone numbers. In this case, the assignment is made when the configuring the stations (i.e., the telephones and subscribers) in the **DID** field. The screen is also visible in this case but not editable.



a) To do this, select an internal call number in the appropriate line from the **Internal Call Number** drop-down list.

b) If subscribers without Internet telephony phone numbers or members of a call group are to be allowed to make external calls via the Internet, the radio button **Use as PABX number for outgoing calls** must be activated. The radio button can be activated for only one single Internet telephony phone number.

23) Click **OK & Next**. You will again see an overview of the possible ITSPs here. The enabled ITSPs are identified with a check mark in the **Enable Provider** column. With Display Status you can check the connection status. If you are having connection problems with an already activated ITSP, you can register it again with **Restart ITSP** on this page.

24) Click **OK & Next**.

25) Enter the upload speed of your Internet connection in the **Upstream up to (Kbps)** field. Please do not confuse this with the download speed!

NOTICE: The number of simultaneous Internet calls permitted is displayed in the **Number of Simultaneous Internet calls** field. If the voice quality deteriorates due to the network load, you will need to reduce the number.

For more information about the number of simultaneous Internet calls, please refer to Limiting the Number of Simultaneous Calls via an ITSP on page 781.

---

26) Click **OK & Next**.

27) Enter the special numbers you want in the **Dialed digits** column.

The following station number entries are valid:

- 0 to 9: allowed digits
- -: Field separator
- X: Any digit from 0 to 9
- N: Any digit from 2 to 9
- Z: One or more digits to follow up to the end of dialing
- C: Simulated dial tone (can be entered up to three times)

28) Use the **Dial over Provider** column to specify whether the special number should be dialed via ISDN or an ITSP. Only the active ITSP is displayed.

NOTICE: Ensure that emergency numbers can always be dialed. If you want to dial emergency numbers via an Internet Telephony Service Provider, you must make sure that the ITSP supports this feature.

---

29) Click **OK & Next**. The status of your ITSP will be displayed.

30) Click **Next** followed by **Finish**. Following this step, please run the **CO Trunk ISDN / Analog / ITSP** wizard to set the prioritization for the exchange line seizure (for example: Exchange Line Seizure First over ITSP and Next over ISDN).

10.2.1.3 How to Configure Multi-Sites over ITSPs

Using the **Multisite Management** wizard, you can define up to 8 sites for the communication system and then assign an ITSP registration and multiple stations to each of them.

Prerequisites

There are as many registrations set up at one or more ITSPs as the number of sites to be configured.

All sites are located within one country.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Multisite Management** wizard.
4) Under **Area Code**, enter an area code for each site (incl. a leading zero, e.g., `069` for Frankfurt and `030` for Berlin). Different area codes or even the same area code may be entered.
5) Under **Area**, enter a name for each site a name (e.g., the cities matching the area codes, i.e., `Frankfurt` and `Berlin`, for example, or department designations such as `Service` and `Sales` if the area code is the same).
6) Assign a route to each site in the **Dedicated Route** selection list. For each ITSP registration, one route is automatically reserved (up to 8 are possible).
7) If you want to delete one or more sites, mark the sites in the **Delete** column and click **Save**.
8) Click **OK & Next**.
9) Assign the stations and groups to the sites:
   a) Mark the desired stations and groups.

NOTICE: You can search for stations and groups by entering a search term in the **Call no**, **DID** or **Name** search fields and then clicking on the magnifying glass icon. You can display all stations and groups by

leaving all search fields empty and then clicking on the magnifying glass icon.

The **Type** option can be used to display all station types (e.g., **SIP Clients** or **System Clients**).

The found stations and groups can be optionally marked individually in the **Selection** column or collectively via the **Select all** check box.

b) Select the desired site under **to Area**.
c) Click **Save**.
d) Repeat the preceding steps for other sites.

10) If required, you can also assign stations and groups of one site to another site:
a) To do this, first select the site from which you want to reassign stations and groups to a different site under **Move selection from area**. All stations and groups of the site are displayed.
b) Select the desired stations either individually in the **Selection** column or collectively via the **Select all** check box.
c) Select the new site under **to Area**.
d) Click **Save**.
e) Repeat the preceding steps for other sites.

11) Click **OK & Next**.

10.2.1.4 How to Save a Preconfigured ITSP Template as a New Template

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Voice Gateway**.
3) In the menu tree, click on **Internet Telephony Service Provider**.
4) Click on the **Add Internet Telephony Service Provider** tab.
5) Select the desired ITSP template from the **Base Template** list.
6) Enter the desired name for the new ITSP template in the **Provider Name** field.
7) Edit the values of the template to suit your needs. An explanation of the values can be found under Voice Gateway>Internet TelephonyService Provider.
8) Click on **Apply** followed by **OK**.

10.2.1.5 How to Customize a Preconfigured ITSP Template

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Voice Gateway**.
3) In the menu tree, click **Internet Telephony Service Provider**.
4) Click on the desired ITSP template in the menu tree.
5) Click on the **Edit Internet Telephony Service Provider** tab.
6) Edit the values of the template to suit your needs. An explanation of the values can be found under Voice Gateway>Internet TelephonyService Provider.

NOTICE: You can reset your edited values to the default values of the template with the **Reset Default Values** button. If the ITSP of the template has already been enabled, all accounts of the ITSP are immediately logged off and re-registered with the default values.

NOTICE: The **Update** button can be used to update the default values in cases where a software update containing more recent default values for this template was performed.

---

7) Click on **Apply** followed by **OK**.

10.2.1.6 How to Manually Update a Preconfigured ITSP Template

Prerequisites

The ITSP of this template is enabled.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Voice Gateway**.
3) In the menu tree, click **Internet Telephony Service Provider**.
4) Click on the desired ITSP template in the menu tree.
5) Click on the **Edit Internet Telephony Service Provider** tab.
6) Make a note of the template values that you have changed as compared to the default values (for example, using a screenshot).
7) Click on **Refresh**. The default values of the template are updated if a software update of the system was performed and if there are more recent default values for this template in that update.
8) Edit the values of the template again to suit your needs. An explanation of the values can be found under Voice Gateway>Internet TelephonyService Provider.

NOTICE: You can reset your edited values to the default values of the template with the **Reset Default Values** button. This causes all accounts of the ITSP to be immediately logged off and re-registered with the default values.

---

9) Click on **Apply** followed by **OK**.

10.2.2 STUN (Simple Traversal of UDP through NAT)

When operating the communication system behind a NAT router, STUN determines its own public IP address/port (which is required for some ITSPs). The functionality is made available on the Internet on STUN servers, whose addresses must be stored in the configuration of the communication system.

The required STUN mode depends on the ITSP infrastructure and the used Internet router. STUN is not required for ITSPs that resolve NAT traversal using infrastructure components in the provider network such as the session border controller.

The following STUN modes can be set at the communication system:

- **Automatic (Default)**

  If no ITSP is active, STUN is fully disabled. With an active ITSP, STUN determines the used firewall type (NAT type) at system startup and detects IP address changes during runtime. Depending on the detected NAT type, STUN changes certain parameters in SIP messages (NAT traversal).

  NOTICE: Symmetric NAT is not supported.

- **Always**

  STUN is always active, for example. Depending on the detected NAT type, some parameters in SIP messages are adapted.
- **Use static IP**

  The DSL modem or Internet router uses a static a static IP address (public IP address), and the ITSP requires a static IP authentication. The static IP address and port that is used by the modem or router must be specified in addition.
- **Port Preserving router**

  The public IP address is determined using STUN. The port is entered in SIP messages unchanged.

10.2.2.1 How to Set the STUN Mode

Prerequisites

You are logged into the WBM with the **Expert** profile.

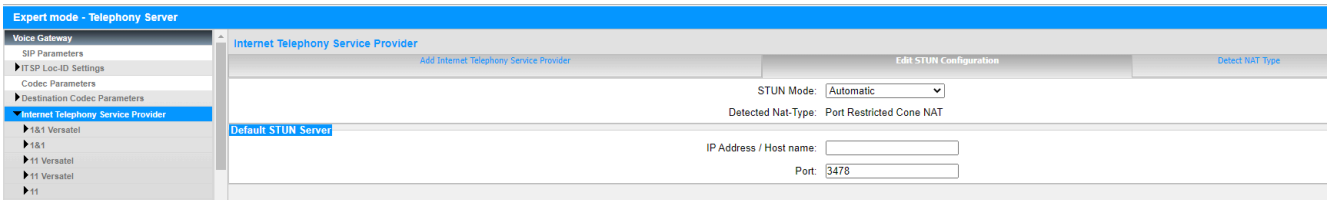
Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click on **Telephony** > **Voice Gateway**.

3) In the menu tree, click **Internet Telephony Service Provider**.

4) Click on the **Edit STUN Configuration** tab.



5) Select the desired STUN mode from the **STUN Mode** drop-down list.
6) If you have selected the STUN mode **Use static IP**, enter the static IP address and the port of the DSL modem or Internet router under **Public IP Address** and **Public SIP Port**, respectively.
7) Click on **Apply**, followed by **OK**.

10.3 CO Access over Digital and Analog Lines

The CO Access over ISDN or analog lines connects the hardware platforms with the public network (PSTN).

Wizards are available to facilitate the configuration of an ISDN outside line or analog outside line.

10.3.1 Trunks

Trunks connect the hardware platforms with the public network (PSTN). Every trunk must be assigned a route through which different properties can be assigned to the trunk.

By default, all trunks are assigned a seizure code and a route. These assignments can be changed by the administrator.

In the case of an ISDN trunk connection, the trunks are also referred to as B-channels.

Trunk code

Using the trunk code, the communication system seizes the specific trunk assigned to that trunk code. The trunk code is also used to program a trunk key or to test a trunk.

MSN Allocation

The service provider assigns one or more MSN (Multiple Subscriber Number) to each ISDN point-to-multipoint (PMP) connection. These can be assigned directly to a line.

System Phone Numbers

System phone numbers include the international prefix, the country code and area code, and the PABX number or one or more MSNs.

ISDN Protocol

The ISDN protocol used depends on the country code. It should only be changed if the PSTN connection explicitly requires some other deviant protocol.

Several protocol templates, which can be adapted to individual requirements, are available. The requisite information for this can be obtained from your Service Provider.

B Channel Seizure Mode

Individual B channels of an ISDN trunk can be blocked for outgoing and/or incoming traffic.

The following B channel seizure modes are possible:

- outgoing only
- incoming only
- outgoing and incoming (default)

The B channel seizure mode is only evaluated when the communication system must offer a B-channel. The applies in the following situations:

S_2 outgoing:	The communication system must offer a B-channel.
S_2 incoming:	The remote station must offer a B-channel. This B-channel is accepted by the communication system without checking the setting. It is thus of no direct significance.
S_0 outgoing:	Since the communication system does not pre-assign a B-channel (any channel), this setting is of no direct significance.
S_0 incoming:	When the remote station sets up a call without specifying a B-channel, the communication system offers a B-channel, while taking the set B channel seizure mode into account.

Dialing Method for Analog CO Trunks (MSI)

The dialing method is automatically detected by the communication system whenever the line is seized. For special cases, the dialing method can also be set directly to Dual Tone Multifrequency (DTMF) or Dial Pulsing (DP).

10.3.1.1 How to Configure an ISDN Outside Line

Use the **CO Trunk ISDN / Analog / ITSP** wizard to configure the ISDN outside line. Depending on which ports are present for CO trunks in the communication system (ISDN or analog), the wizard goes through different steps.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The communication system is connected to an ISDN trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **CO Trunk ISDN / Analog / ITSP** wizard. The wizard displays an overview of the box(es), slot(s) and S_0 ports.

4) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
5) Enter the local area code, e.g., 89 for Munich, in the **Local area code** field.
6) For point-to-point connections, enter the system phone number of your trunk connection, e.g., 7007 (your connection number) in the **PABX number** field.
7) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., `00-1` for calls from Germany to the USA and `011-49` for calls from the USA to Germany.
8) Click on **OK & Next**.
9) Select one of the following connection types for the relevant connection (box, slot and S_0 port):

   - If you want to configure a point-to-point connection, select the **Point-to-point connection** radio button.
   - If you want to configure a point-to-multipoint connection, select the **Point-to-multipoint connection** radio button.
10) Click on **OK & Next**.
11) If a point-to-multipoint connection is involved, enter the MSN for the relevant connection (box, slot and S_0 port) and click **OK & Next**.
12) Leave the setting of the **No call via Internet** check box unchanged and click **Skip**.
13) Select the preferred trunk (CO) access in the **First over** drop-down list and then click **OK & Next**.
14) Click on **OK & Next** followed by **Finish**.

10.3.1.2 How to Configure an Analog Outside Line

Use the **CO Trunk ISDN / Analog / ITSP** wizard to configure the analog outside line.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Your communication system is connected to an analog trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **CO Trunk ISDN / Analog / ITSP** wizard. The wizard displays an overview of the box(es), slot(s) and analog ports.
4) In the **Country Code** field, enter the country code prefix, e.g., `49` for Germany or `1` for the U.S.
5) Enter the local area code, e.g., 89 for Munich, in the **Local area code** field.
6) For point-to-point connections, enter the system phone number of your trunk connection, e.g., 7007 (your connection number) in the **PABX number** field.

7) Change the **International Prefix** field only if required. The applicable values for Germany and the United States are `00` and `011`, respectively.

   For international calls, the phone number is preceded by the international prefix and the country code, e.g., `00-1` for calls from Germany to the USA and `011-49` for calls from the USA to Germany.
8) Click on **OK & Next**.
9) Click on **Skip ISDN**.
10) Leave the setting of the **No call via Internet** check box unchanged and click **Skip**.
11) Select the protocol for displaying the phone number (service provider dependent) from the **Protocol** drop-down list:
    - If you want to use Frequency Shift Keying, select **FSK**.
    - If you want to use Dual Tone Multifrequency (DTMF), select **DTMF**.
    - If you do not want to use station number display (calling line ID), select **None**.
12) Click on **OK & Next**.
13) Click on **Edit** to configure the properties of the relevant trunk. If required, edit the values for the **Dialing method**, **CO call identification**, **Flash**, **Line Length** and **Flags** and then click **OK**.
14) Click on **OK & Next**.
15) Click on **Skip** and then, if necessary, on **OK & Next**.
16) Select the preferred trunk (CO) access in the **First over** drop-down list and then click **OK & Next**.
17) Click on **OK & Next** followed by **Finish**.

10.3.1.3 How to Display All Trunks

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click on **Trunks/Routing** > **Trunks** in the menu tree. Depending on the configuration of the communication system, all possible trunks, including the trunk code and route, will be displayed.

10.3.1.4 How to Display Individual Trunks

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.

3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired line. The trunk connected to the communication system, including the trunk code and route, will be displayed.
4) Click on **OK**.

10.3.1.5 How to Change the Trunk Code

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired line.
4) Click on the **Change Line** tab.
5) Enter the desired value in the **Code** field.

NOTICE: If no value is entered as the code, this trunk has no trunk code.

---

6) Click on **Apply** followed by **OK**.

10.3.1.6 How to Assign an MSN to a Trunk

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.
3) Click **Trunks/Routing** > **MSN assign** in the menu tree.
4) Click on the entry that you want to edit under **MSN assign** in the menu tree.
5) Enter the **MSN**.
6) Select the route that you want to assign from the **Trunk** drop-down list.
7) Click on **Apply** followed by **OK**.

10.3.1.7 ISDN protocol, modify

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.

3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired port.
4) Click on the **Change ISDN Flags** tab.
5) Select the desired protocol from the drop-down list in the **Protocol: Description** area.
6) Click on **Apply** followed by **OK**.

10.3.1.8 How to Change the B Channel Seizure Mode

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.
3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired port.
4) Click on the **Change B-Channel** tab.
5) Clear the check boxes for each channel in the **outgoing** and **incoming** columns as desired.
6) Click on **Apply** followed by **OK**.

10.3.1.9 How to Change the Dialing Method

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.
3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired port.
4) Click on the **Edit MSI Flags** tab.
5) Set the dialing method to Dual Tone Multifrequency (DTMF) or Dial Pulsing (DP).
6) Click on **Apply** followed by **OK**.

10.3.2 Routes

Routes enable trunks (B channels) to be grouped. Separate parameters can be configured for each trunk group (= route).

Each trunk can be assigned to exactly one route. By default, all trunks are assigned to route 1.

For each route, a name and a seizure code can be assigned.

INFO: Seizure codes only work for outgoing trunk seizures if LCR has not been activated.

B Channel Allocation

The allocation of B channels to different trunk groups is also called B-channel allocation. For ISDN trunk connections with multiple B-channels, e.g., S_{2M} ports, it may be useful to allocate B channels to different trunk groups (called B-channel allocation).

For outgoing calls, only B-channels that are included in the trunk group can be selected (e.g., trunk group selected via the seizure code, overflow trunk group or trunk group selected using LCR)

Incoming calls are always accepted, regardless of the trunk group. As a rule, the B-channel offered by the peer is seized. Consequently, the B-channel allocation configured in the system must also be supported on the peer side (system or public network). If this is not the case, the correct allocation of the call to the correct trunk group cannot be guaranteed.

Trunk group key

A subscriber can program a trunk group key on the telephone. One trunk group key is reserved for outbound calls. Calls placed via trunk group keys are subject to COS toll restriction levels and rules.

When a subscriber presses a trunk group key (or dials a seizure code), the communication system seizes an available trunk that is assigned to the appropriate route. The telephone shows the trunk number in the display. If all trunks of the route are seized, the corresponding LED lights up, even in the case of a successful overflow.

Overflow Route with LCR Disabled

For each route, the administrator can also define an overflow route. If all the trunks of a route are busy during a seizure attempt, the search for trunks continues among all trunks in the overflow route. If all the trunks in the overflow route are busy as well, no further overflow occurs.

Overflow Route with LCR Enabled

As part of the LCR configuration, the administrator configure up to 16 entries per route table that are then processed sequentially within the context of an overflow.

Type of Seizure

For an outgoing route seizure, the administrator can specify the criteria to be used by the communication system when searching for an available trunk in the required direction. This is done by defining the type of seizure as follows:

- cyclic:

  after the last outbound seized trunk - search begins at the next higher trunk number, as of the last outgoing trunk reserved for that direction. Consequently, all trunks are used with similar frequency.
- linear:

  always the first free trunk - search begins at the lowest trunk number assigned to that route.

Entering a PABX Number, Incoming and Outgoing

The administrator can configure the PABX number incoming and the PABX number outgoing separately. Thus, the own number for outgoing calls can be represented differently than is needed for accessibility by incoming calls. The portions for the country code, local area code and the PABX number must each be entered separately in this case. Different entries for the PABX number incoming and outgoing require the availability of the "CLIP no screening" feature at the Central Office. If no PABX number outgoing is configured, the communication system always uses the data of the PABX number incoming.

In the case of an incoming seizure on an ISDN line, the communication system truncates the PABX number portion (left-aligned) from the received phone number in accordance with the incoming phone number type (Type Of Number = TON, see table below Caller ID) and interprets the remaining portion as the Direct Inward Dialing number. For call number information to the PSTN, the communication system automatically inserts the outgoing PABX number portion as the leading portion of the call number in accordance with the configured type of number (TON). In Germany, the PABX number portion must be specified at the trunk connection without the local area code and the intercept code (0).

Station Number Transmission

The station number that is sent to the PSTN and to the receiver can be composed as follows:

Type Of Number (TON), outgoing	Station number transmitted to the PSTN
Unknown TON = Unknown	only DID number (default setting)
PABX number TON = Subscriber	PABX number + DID number
Local area code TON = National	+ Local area code + PABX number + DID number
Country code TON = International	Country code + Local area code + PABX number + DID number
Internal TON=Internal	Only for networked system: number prefixes may not be added for closed numbering plans. Call number prefixes are suppressed here.

In addition, you can specify which call number information is to be transmitted from the dialing station to the destination station.

Call number type	Call number transmitted to the PSTN
Internal	In this case, only the internal call number is transmitted. If the destination is an external station, either no number is transmitted or only that of the Attendant Console. The internal call number can be displayed when the destination is an internal station.
Direct inward dialing	In this case, only the DID number is transmitted. The internal call number is not provided for display at internal destinations in other nodes. The call number information is sufficient for external destinations.
Internal / DID	This setting is useful for networking purposes. Both the internal call number and the DID call number are transmitted to the destination station. If an internal station is called within the network, the internal call number of the caller can be displayed for this station. If the internal destination station has activated call forwarding to an external destination, for example, a DID number can also be transmitted in this case.

In addition, the desired handling of the route prefix can be configured:

- Incoming call

  The caller's number is supplemented with the seizure code (-> dialable format for callback) or passed through transparently when it is transmitted to the S0 bus. Default: enabled.
- Outgoing call

  The display of the dialed phone number on the system telephone occurs with or without the route prefix. Default: enabled.

Second CO Code

A second trunk code (CO code) is defined if the communication system is a subsystem of another communication system or is networked with several other communication systems. It is only relevant for networking routes (route type = PABX). In this case, the second trunk code is the seizure code for the main system. Within a network, the codes for the trunk seizure, the route seizure code(s) and the second CO code must be configured uniformly. The default in Germany is 0.

10.3.2.1 How to Change a Route Assignment

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Navigate in the menu tree under **Trunks/Routing** > **Trunks** > **...** to the desired line.
4) Click on the **Change Line** tab.

5) Select the route that you want to assign to the trunk from the **Routes** drop-down list.
6) Click on **Apply** followed by **OK**.

10.3.2.2 How to Change the Route Name

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the entry that you want to edit under **Route** in the menu tree.
5) Enter the desired value in the **Route Name** field.
6) Click on **Apply** followed by **OK**.

10.3.2.3 How to Change the Seizure Code

Prerequisites

You are logged into the WBM with the **Expert** profile.

NOTICE: Seizure codes only work if LCR has not been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the entry that you want to edit under **Route** in the menu tree.
5) Enter the desired value in the **Seizure code** field.
6) Click on **Apply** followed by **OK**.

10.3.2.4 How to Configure an Overflow Route with LCR Disabled

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.
3) Click **Trunks / Routing** > **Route** in the menu tree.
4) Click on the entry that you want to edit under **Route** in the menu tree.

5) Select the desired item from the **Overflow route** drop-down list.
6) Click on **Apply** followed by **OK**.

10.3.2.5 How to Configure an Overflow Route with LCR Enabled

When LCR is enabled, overflow treatment is performed by processing the individual entries of an LCR table successively in the context of the LCR configuration (see LCR (Least Cost Routing)).

10.3.2.6 How to Configure the Type of Seizure

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.
6) In the **Type of seizure** drop-down list, select either **cyclic** or **linear**.
7) Click on **Apply** followed by **OK**.

10.3.2.7 How to Enter the PABX Number Incoming and Outgoing

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks / Routing**.
3) Click **Trunks / Routing** > **Route** in the menu tree.
4) Click on the entry that you want to edit under **Route** in the menu tree.
5) In the **PABX number incoming** area, enter the appropriate values without leading zeros in the fields **Country Code**, **Local area code** and **PABX number**.
6) In the **PABX number Outgoing** area, enter the appropriate values without leading zeros in the fields **Country Code**, **Local area code** and **PABX number**.
7) Select one of the following options:
   - If you want to suppress the station number, enable the **Suppress station number** check box.
   - If you do not want to suppress the station number, leave the **Suppress station number** disabled.
8) Click on **Apply** followed by **OK**.

10.3.2.8 How to Configure the Format of the Transmitted Call Number

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.
6) Select the desired format of the transmitted call number from the **No. and type, outgoing** drop-down list.
7) Click on **Apply** followed by **OK**.

10.3.2.9 How to Configure the Type of the Transmitted Call Number

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.
6) In the **Call number type** drop-down list, select the item **Internal**, **Direct inward dialing** or **Internal/DID**.
7) Click on **Apply** followed by **OK**.

10.3.2.10 How to Configure the Direction Prefix

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.

6) Select one of the following options:
   - If you want the seizure code to be added to the Calling Line ID for inbound calls, select the check box **Add direction prefix incoming** in the **Routing flags** area.
   - If you do not want the seizure code to be added to the Calling Line ID for inbound calls, clear the check box **Add direction prefix incoming** in the **Routing flags** area.
   - If you want the seizure code to be added to the Calling Line ID for outbound calls, select the check box **Add direction prefix outgoing** in the **Routing flags** area.
   - If you do not want the seizure code to be added to the Calling Line ID for outbound calls, clear the check box **Add direction prefix outgoing** in the **Routing flags** area.
7) Click on **Apply** followed by **OK**.

10.3.2.11 How to Define a Route for Networking and Enter a Second CO Code

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the entry that you want to edit under **Route** in the menu tree.
5) Enter the desired value in the field **CO code (2nd trunk code)**.
6) Click on the **Change Routing Parameters** tab.
7) Select the item **PABX** in the **Route type** drop-down list.
8) Click on **Apply** followed by **OK**.

10.3.3 Dial Tone Monitoring

When setting up a connection over an analog trunk line, the dialed digits can be sent to the Central Office only when a dial tone (audible signal) has been detected. Since the time until the arrival of the dial tone varies depending on the network provider and network state, the arrival of the dial tone can be monitored.

The dial tone monitoring time and the digit dialing time are configured using Manager E.

Delay Period for Dial Tone Monitoring

The monitoring of the dial tone can be done immediately or only after a pause. In some cases, additional tones may need to be played back to the subscriber after the line is seized, for example, to inform him or her that call forwarding has been enabled at the Central office. For such cases, a delay period for the dial tone monitoring (Analog trunk seizure, 1-9 seconds) can be programmed. The dialed digits will then be sent to the CO only after this pause.

NOTICE: Notes for Brazil:

If the DTMF dialing method is used from analog phone devices in conjunction with analog trunks (TLAx and TML8W) and pulse dialing after the dial tone monitoring, problems may arise with toll restriction when the country code is set to Brazil. In this case, the DTMF signals from the analog devices go directly to the analog trunk lines. All DTMF signals that were dialed before receiving the dial tone are lost. Consequently, for such cases, least cost routing (LCR) must be enabled for the dialing method and toll restriction to operate properly at the device.

Dial tone monitoring time

This parameter indicates how long the system will wait for the dial tone and is configurable. If no dial tone is detected during the configured dial tone monitoring time, the line is taken out of service. The system checks at cyclical intervals whether the dial tone is once again present. If this is the case, the line in question is put back into operation.

Digit dialing time

This parameter defines how many seconds after detection of the dial tone the first dialed digit is to be sent to the Central Office (default setting: 0 s).

Analysis of the Second Dial Tone

The communication system can recognize an additional dial tone (2nd dial tone). This is relevant for public network providers who transmit at a second dial tone for international calls, e.g., for Belgium after 00 and for France after 16 or 19. For Germany, this feature is not relevant.

10.3.3.1 How to Configure a Delay Period for Dial Tone Monitoring

Prerequisites

An analog port with the analog outside line is available.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the analog route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.
6) If the dial tone monitoring is to take place immediately, enable the radio button **no pause** in the **Analog trunk seizure** area.
7) If the dial tone monitoring is to take place only after a delay period, select the delay period in seconds in the **Analog trunk seizure** area.
8) Click on **Apply** followed by **OK**.

10.3.3.2 How to Configure the Dial Tone Monitoring Time

Prerequisites

An analog trunk board is plugged in.

Step by Step

1) Log into Manager E at the admin PC.
2) Click on **File | Transmit** in the menu bar.
3) Select the **Communication** tab.
4) In the **Access** area, enable the appropriate radio button, depending on the type of connection from the admin PC to the communication system.
5) Enable the radio button **Read/write CDB** and click on **System -> PC**.
6) Click on **OK**. The CDB will be transferred from the communication system to Manager E.
7) After the successful transfer, click **OK** and then on **Close**.
8) Click in Manager E in the menu tree of the system view on **Settings** > **System Parameters** > **Time Parameters**.
9) In the list below **Dial tone monitoring time**, set the maximum time to wait for a dial tone under **Base** and **Factor** (default = base `1s`, Factor = `10`).
10) Click on **Apply**.
11) Click on **File | Transmit** in the menu bar.
12) Select the **Communication** tab.
13) Click on **PC > System** followed by **OK**. The settings are transferred to the communication system.
14) Then click **OK** and **Close**.

10.3.3.3 How to Configure the Digit Dial Time

Prerequisites

An analog trunk board is plugged in.

Step by Step

1) Log into Manager E at the admin PC.
2) Click on **File | Transmit** in the menu bar.
3) Select the **Communication** tab.
4) In the **Access** area, enable the appropriate radio button, depending on the type of connection from the admin PC to the communication system.
5) Enable the radio button **Read/write CDB** and click on **System -> PC**.
6) Click on **OK**. The CDB will be transferred from the communication system to Manager E.
7) After the successful transfer, click **OK** and then on **Close**.
8) Click in Manager E in the menu tree of the system view on **Settings** > **System Parameters** > **Time Parameters**.
9) In the list below **Time between HT analysis and dialing of trunk main station interface**, set the time under **Base** and **Factor** to specify how many seconds after the detection of the dial tone, the first dialed digit is to be sent to the Central Office (default: Base = `10 ms`, Factor = `0`).

10) Click on **Apply**.
11) Click on **File | Transmit** in the menu bar.
12) Select the **Communication** tab.
13) Click on **PC > System** followed by **OK**. The settings are transferred to the communication system.
14) Then click **OK** and **Close**.

10.3.3.4 How to Enable or Disable the Analysis of the Second Dial Tone

Prerequisites

An analog port with the analog outside line is available.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click **Trunks/Routing** > **Route** in the menu tree.
4) Click on the analog route that you want to edit under **Route** in the menu tree.
5) Click on the **Change Routing Parameters** tab.
6) If you want to enable the analysis of the second dial tone, select the **Analysis of second dial tone** check box in the **Routing flags** area.
7) If you want to disable the analysis of the second dial tone, clear the **Analysis of second dial tone** check box in the **Routing flags** area.
8) Click on **Apply** followed by **OK**.

10.4 Prioritizing the Exchange Line Seizure with LCR Enabled

The prioritization for exchange line seizure defines in what order different network providers (ISDN/analog or ITSPs) are selected.

The exchange line seizure normally occurs by dialing the prefix "0". Within this code, different providers are prioritized (depending on what is preset). For example, an outbound call may be first routed via an ITSP and, if the exchange line seizure fails, be then sent via ISDN.

10.4.1 How to Prioritize the Seizure of Exchange Lines

The **CO Trunk ISDN / Analog / ITSP** wizard can be used to configure the order in which exchanges lines are seized over ISDN/analog providers and ITSPs.

Prerequisites

You are logged on to the WBM with the **Advanced** profile. Different ITSPs have been set up.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **CO Trunk ISDN / Analog / ITSP** wizard. The wizard displays an overview of the box(es), slot(s) and analog ports.
4) Click on **OK & Next**.
5) Continue clicking on **OK & Next** as often as needed until you reach the **Prioritization for Exchange Line Seizure** window.
6) In the **Try to get 'Outside line Seizure'** area, select the preferred network provider over which the communication system should first try to obtain a free CO trunk (i.e., an exchange line) from the **First over** drop-down list.
7) Then select a second network provider over which the next attempt to seize an exchange line should be made from the **Next over** drop-down list.
8) Finally, select a third network provider over which an attempt to seize an exchange line should be made from the following **Next over** drop-down list.
9) Click on **OK & Next** followed by **Finish**.

11 Stations

A subscriber or station is a communication partner connected to the communication system. In general, every station (apart from virtual stations) is assigned a terminal. A terminal is, for example, a telephone, a PC or fax device. The stations may also be users of the UC Clients.

The following types of stations exist:

- IP stations (also known as IP clients)
- SIP stations (a subset of IP stations)
- UP0 stations
- DECT stations
- Mitel SIP-DECT stations
- ISDN stations
- Analog stations
- Mobility stations (mobile stations, see Mobility)
- Virtual stations

The data of subscribers (name, station number, DID number, e-mail address, etc.) can be imported as an XML file during the initial installation (see Individual Dial Plan). In addition, the subscriber data can also be exported to an XML file (see Exporting Subscriber Data).

Licensing Procedure for Stations

All stations are subject to licensing. To begin with, stations can be set up during the initial installation or later by using the Station wizards. After a successful setup, the subscribers can make internal calls. In the next step, the station licenses must be activated and assigned to the stations. Once the licenses have been assigned successfully, the subscribers can also make external calls.

Related concepts

Licensing on page 282
Mobility on page 898

11.1 Dial Plan

A dial plan, which is also called a numbering plan, is a list of all phone numbers and codes available in the communication system. It includes, among other things, the internal call numbers, DID numbers and group call numbers. In the communication system, the call numbers and codes are preset with default values. However, these values can be adapted to suit individual requirements as needed.

When setting up call numbers or codes, error messages may be produced if the desired number is already being used. The dial plan can be used to check which call numbers can still be assigned.

11.1.1 Default Dial Plan

The default dial plan includes all call numbers and codes that are predefined n the communication system with default values.

These default values can be edited as necessary. Some numbers can be also deleted completely so that they no longer appear in a dial plan overview.

Default dial plan for the hardware platforms and the softswitch:

Type of call numbers	X1	X3/X5/X8/S	Action
Internal station numbers	11-30	100-742	deletable
User direct inward dialing numbers	11 -30	100-742	deletable
Group call numbers 1-90 Group call numbers 91-800	31-40 -	350-439 not preset	deletable
Trunk station number	700-703	from 7801 onward	deletable
Seizure codes (external codes): Trk. Grp 1 (trunk: ISDN, analog) Rte. 8 (UC Suite) Trk. Grp 12-15 (trunk: ITSP) Rte. 16 (Networking)	 0 = World / 9 = USA - not preset not preset	 0 = World / 9 = USA 851 855-858 859	only editable
Attendant code (Intercept position), Internal	9 = World 0 = USA	9 = World 0 = USA	only editable
Attendant code (Intercept position), Direct inward dialing	0 = ROW – = USA	0 = ROW – = USA	only editable
Station numbers for online users	not preset	749	only editable
Call number for remote access	not preset	not preset	only editable
Call number for voicemail UC Smart UC Suite	351 -	351 not preset	only editable only editable
Conference call numbers	-	not preset	only editable
Call number for parking	-	not preset	only editable
AutoAttendant numbers	-	not preset	only editable
Station number for Attendant Console	9 = World 0 = USA	9 = World 0 = USA	only editable
Substitution for "#" (for service codes)	75	75	deletable

Type of call numbers	X1	X3/X5/X8/S	Action
Substitution for "#" (for service codes)	76	76	deletable
Service codes			only editable

11.1.2 Individual Dial Plan

The communication system allows you to set up an individual dial plan by editing the default values of the call numbers and codes. A reload of the communication system resets the values to the defaults.

The following actions are useful for this purpose:

- Delete defaults: apart from some exceptions (special default numbers), default call numbers can be deleted. These call numbers are identified as "deletable" in the "Action" column of the default dial plan table.
- Edit special defaults: these call numbers must not be deleted. However, their values may be edited. These call numbers are identified as "only editable" in the "Action" column of the default dial plan table.
- Import call numbers and station data: station data can be imported via an XML file during the initial installation. The call numbers and DID numbers of the stations are imported as well. This is usually performed during the initial installation.

Importing Station Data via an XML File

An individual dial plan can be imported into the communication system via an XML file in UTF-8 format during the initial installation.

The OpenScape Business Assistant administration program makes the file `csv-templates.zip` available under **Service Center** > **Documents** > **CSV Templates**. This zip file contains, among other things, the following files, including descriptions:

- `portdata_xml_import_empty.xml`

  This template contains registers without sample records. New records can be entered using Microsoft Excel, for example.
- `portdata_xml_import_example.xml`

  This template contains registers with sample records. These records can be edited using Microsoft Excel, for example. Data records that are no longer needed should be deleted.
- `portdata_xml_import_syntax.txt`

  Descriptions in German and English on how to create records correctly.

11.1.2.1 How to Delete or Edit Default Phone Numbers

You can delete some of the default call numbers and then redefine them via the wizards. For special default call numbers, you can edit and change the default values.

Prerequisites

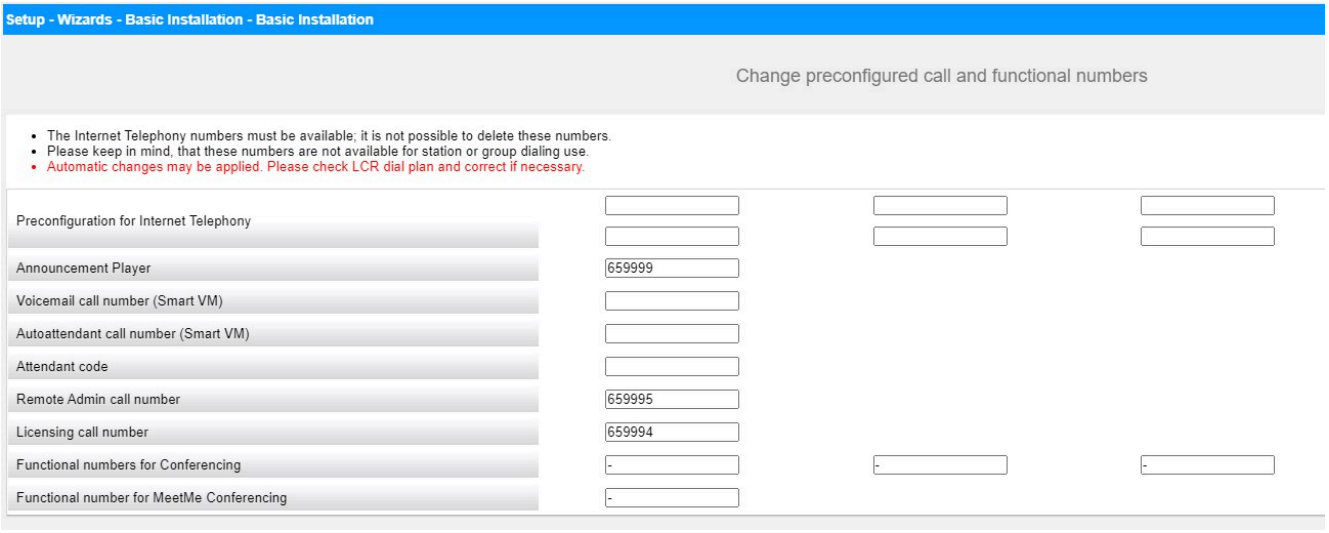
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Basic Installation** wizard.
3) Click on **Next**.

> **NOTICE:** You can have an overview of all configured station numbers displayed by enabling the radio button **Display station configuration** and then clicking **Execute function**.

4) Enable the radio button **Delete All station call numbers**.
5) Enable the check box **Delete all station call numbers** in the confirmation prompt.
6) Click on **Execute function**.



7) Edit the default values in the fields of the special default call numbers if required.
8) Click on **OK**. The call numbers are deleted, and any other changes made to the special default call numbers are applied.
9) Click on **Abort** to end the **Basic Installation** wizard.

11.1.2.2 How to Edit Special Default Call Numbers

You can change the predefined call numbers for special functions.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

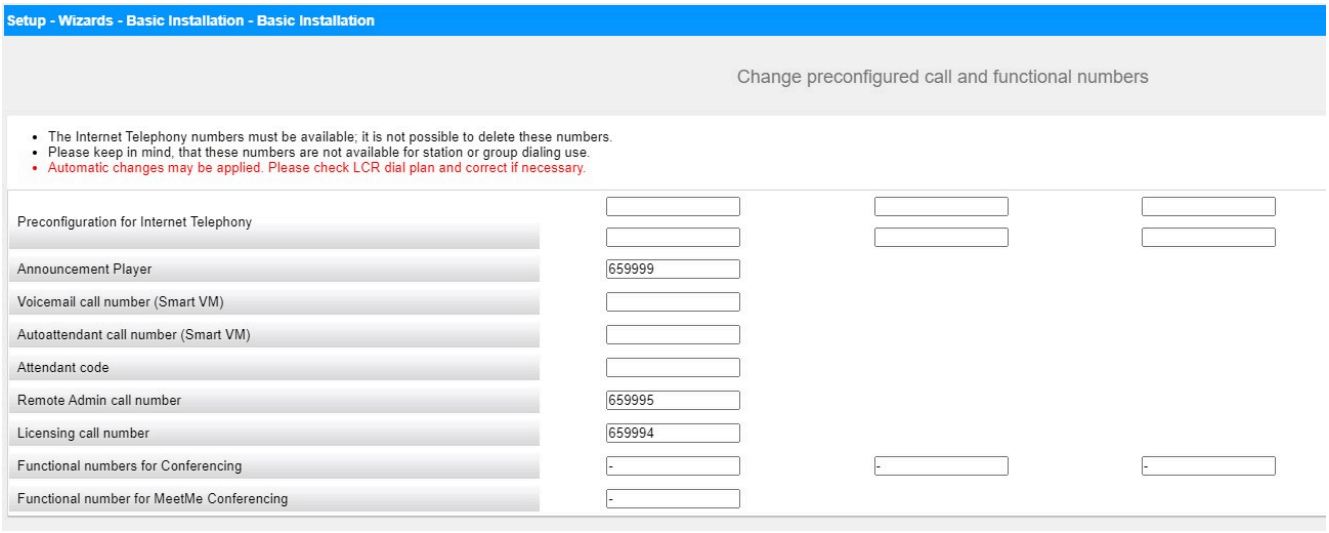
Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Basic Installation** wizard.

3) Click on **Next**.

NOTICE: You can have an overview of all configured station numbers displayed by enabling the radio button **Display station configuration** and then clicking **Execute function**.

4) Enable the radio button **Change pre-configured call and functional numbers**.
5) Click on **Execute function**.



6) Enter the desired call numbers and codes in the fields and click **OK**. The new call numbers and codes are saved.

NOTICE: Note that the call numbers configured here cannot be assigned as station numbers, DID numbers or group call numbers.

7) Click on **Cancel** to end the **Basic Installation** wizard.

11.1.2.3 How to Import Call Numbers and Station Data

You can import predefined station data via an XML file you created earlier.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

An XML file with the entered data is available in UTF-8 format. An XML template can be found under **Service Center** > **Documents** > **CSV Templates**.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Basic Installation** wizard.

3) Click **Next**.

NOTICE: You can have an overview of all configured station numbers displayed by enabling the radio button **Display station configuration** and then clicking **Execute function**.

4) Enable the radio button **Import XML file with station data**.
5) Click on **Execute function**.
6) Use **Browse** to select the created XML file and click **Open**.
7) Click **OK** when finished. The station data is imported.
8) Click **Cancel** to end the **Basic Installation** wizard.

11.2 LAN Telephony Requirements

The term LAN telephony refers to the communication between IP stations in an internal network (LAN). To ensure the quality of the voice transmission in LAN telephony, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

To guarantee loss-free transmission and good voice quality, voice signals are digitized using audio codecs and marked using special procedures (Quality of Service) so that voice transmission has priority over data.

Requirements

- LAN with at least 100 Mbps and full duplex
- Every component in the IP network must be connected to a separate port on a switch or to a router; a hub should not be used.
- Not more than 50 msec delay in one direction (One Way Delay); not more than 150 msec total delay
- Max. 3% packet loss; if a fax/modem via G.711 is used, the packet loss must not exceed 0.05%.
- Not more than 20 msec jitter
- Support for Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) or ToS (RFC 791)
- Maximum 40% network load

11.2.1 Audio Codecs

An audio codec is a program that encodes and decodes voice in digital data packets (IP packets). The data compression rate can vary depending on the audio codec used. The bandwidth requirement for transferring an IP packet is lower if the packet is compressed. The decoding of data packets can, however, have a negative impact on voice quality and the playback continuity.

The recipient and sender must use the same codec to ensure that the data can be correctly decoded back into voice after transport.

Supported Audio Codecs

The following audio codecs are supported:

- G.729A, G.729AB: voice encoding at 8 Kbps - good voice quality.
- G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN).

The audio codecs can be assigned priorities between 1 (high) and 4 (low). The communication automatically tries to use the audio codec with the highest priority available for every connection. Using an audio codec with low voice compression (good voice quality) increases network load. In the case of intensive IP telephony, this can lead to diminished voice quality in a network already overloaded by data transfers.

The communication system can enable voice activity detection (VAD) for certain codecs. This can reduce network load during long voice pauses.

You can specify a frame size (IP packet size) of 10 to 90 msec for every codec. This specifies the sampling rate at which the audio codec splits the voice signal into IP packets. While a higher value (90 msec, for instance) results in a better relationship between payload and the IP packet overhead, it also increases the transfer delay.

It is possible to disable the resource-hungry G.729 codecs and to only use the G.711 codecs. This optimizes the number of possible simultaneous calls. If this function is enabled, the system must be restarted.

In OSBiz X systems, payload ends in the system, so the users talk with a codec, which is supported by the system. For example, HFA phone has firstly set G.722 codec. The system does not support G.722 codec and G.711 codec has been set as its first option. In this case, the two users will talk with G.711 codec. Regarding OSBiz S systems, the users talk with G.722 codec, while there is end-to-end payload.

11.2.1.1 How to Configure Audio Codec Parameters

Prerequisites

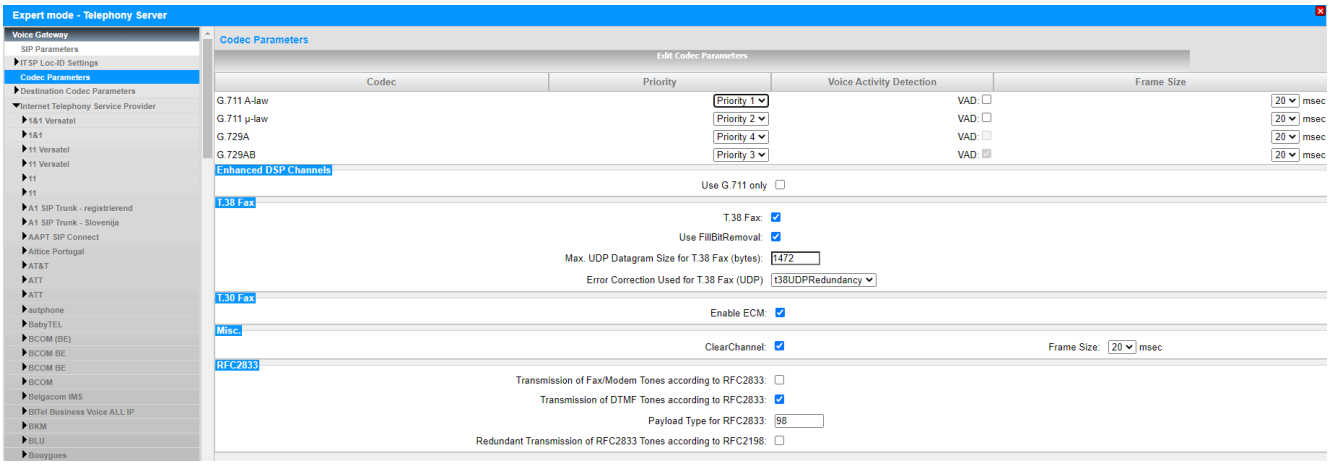
You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony Server** > **Voice Gateway**.

3) In the menu tree, click **Codec Parameters**.



4) Assign priority 1 (high) through 4 (low) to the required audio codecs via the **Priority** drop-down list.
5) Activate or deactivate the radio button **Voice Activity Detection (VAD)** for the desired audio codecs.
6) Use the **Frame Size** field for the desired audio codecs to define the frame size into which the audio codec splits the IP voice packets.

NOTICE: You must enter the same value for all codecs, e.g. 20 msec. It is not supported to configure different values for each codec.

---

7) If you want to use only the two G.711 audio codecs, select the **Use G.711 only** check box in the **Enhanced DSP Channels** area.
8) Click on **Apply**, followed by **OK**.

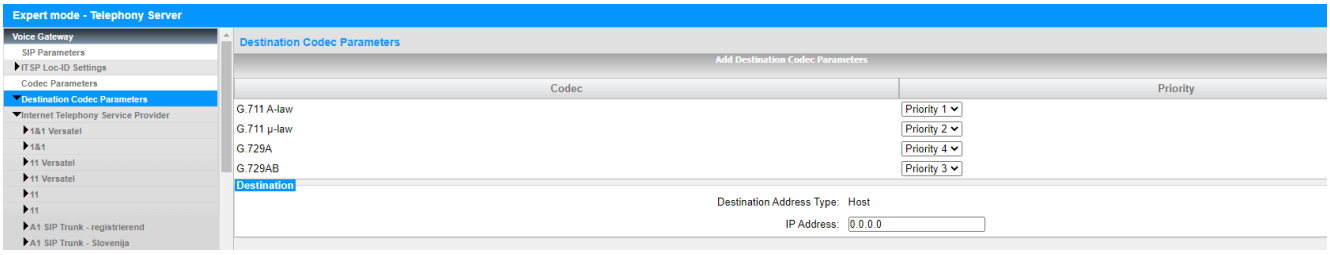
11.2.1.2 How to Assign Audio Codec Parameters to a Destination

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Voice Gateway**.
3) In the menu tree, click **Destination Codec Parameters**.



4) Assign priority 1 (high) through 4 (low) to the required audio codecs via the **Priority** drop-down list.

5) Under **IP address**, enter the IP address of the destination to which the previously set priorities of the audio codec are to be assigned (for example, `192.168.1.10`).
6) Click on **Apply** followed by **OK**.

11.2.2 Transmission of Tones According to RFC 2833

The transmission of DTMF tones and fax/modem tones according to RFC 2833 can be enabled or disabled.

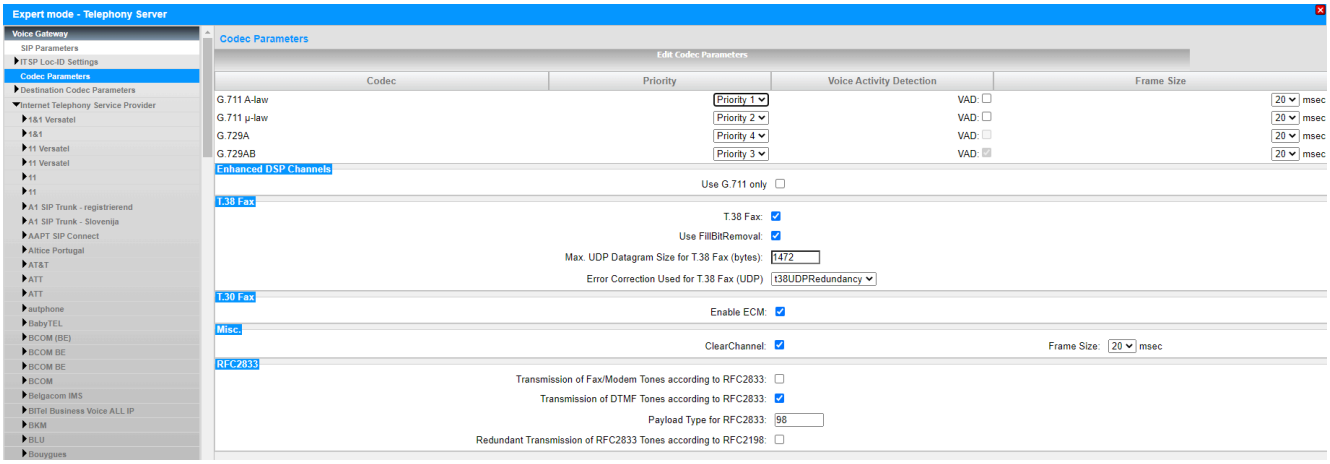
11.2.2.1 How to Enable or Disable Transmission of Fax/Modem Tones According to RFC2833

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Voice Gateway**.
3) In the menu tree, click **Codec Parameters**.



4) Select one of the following options:
   - If you want to enable the function, select the **Transmission of Fax/ Modem Tones according to RFC2833** check box.
   - If you want to disable the function, clear the **Transmission of Fax/ Modem Tones according to RFC2833** check box.
5) Click on **Apply** followed by **OK**.

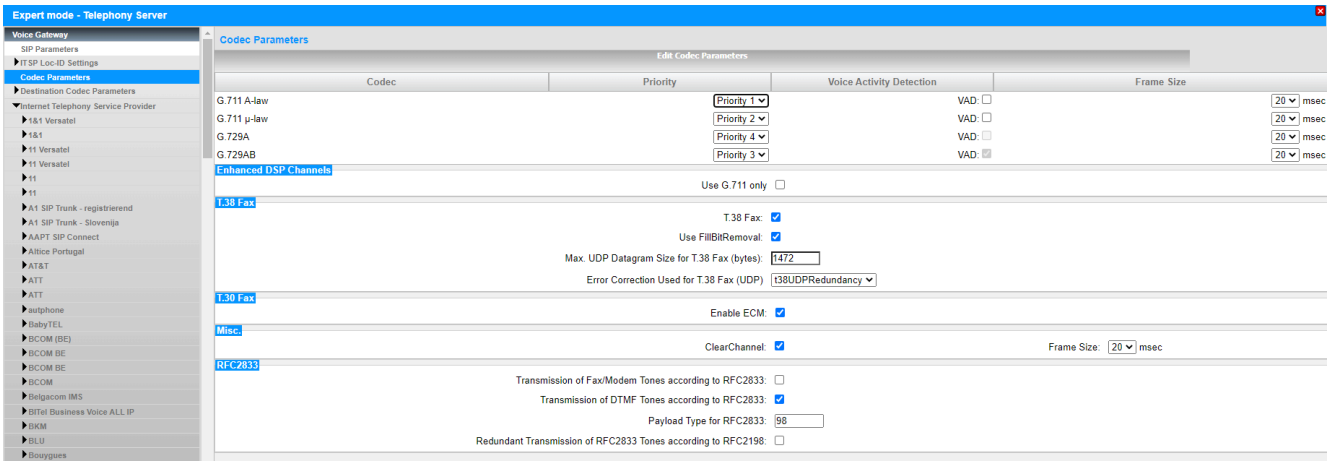
11.2.2.2 How to Enable or Disable Transmission of DTMF Tones According to RFC2833

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Voice Gateway**.
3) In the menu tree, click **Codec Parameters**.



4) Select one of the following options:
   - If you want to enable the function, select the **Transmission of DTMF Tones according to RFC2833** check box.
   - If you want to disable the function, clear the **Transmission of DTMF Tones according to RFC2833** check box.
5) Click on **Apply** followed by **OK**.

11.2.3 Quality of Service

Quality of Service (QoS) encompasses various procedures for guaranteeing the highest possible quality and integrity during the transmission of data packets (IP packets). For good voice quality during voice transmission, QoS is used in the IP network to give IP voice packets priority over IP data packets from other applications.

The IP packets are assigned a special marker (code point) for prioritization. Categorization in different classes is performed based on priority information. If the components available in the IP network (communication system, SIP stations, and Internet routers, for instance) support QoS, you can assign different bandwidth to these classes and thus transport the IP voice packets first.

Priority Classes According to DiffServ

For DiffServ-based prioritization, different code points are defined for the Type of Service (ToS) field so that IP-packet transmission can be split into different classes.

- Expedited Forwarding (EF) Code point: guarantees constant bandwidth. The bandwidth is always the same for IP packets marked with this code point. Once the set value is reached, all IP packets that exceed this bandwidth are dropped.
- Assured Forwarding (AF) Code point: guarantees minimum bandwidth. IP packets that are marked with this code point have a lower priority than

EF and must share the bandwidth not used by EF. Once the set value is reached, all IP packets that exceed this bandwidth are rejected.

Four classes are reserved for AF: AF1x (low priority), AF2x, AF3x and AF4x (high priority), where "x" stands for one of three dropping levels: low (1), medium (2) and high (3). In the case of "low", packets are buffered over an extended period, in the case of "high", packets are promptly rejected if they cannot be forwarded.

- Best Effort (BE): Unmarked IP packets (Type of Service (ToS) field=00) are handled in the same way as the lowest priority.

Priority Classes According to IP Precedence

In addition to the DiffServ method, there are several older definitions, which perform the prioritization based on the ToS field. To achieve the best possible adaptation of the communication system to any required settings in the customer network, classes 3 to 7 (CS3-CS7) can be selected for IP Precedence, for example.

Individual Priority Classes

If none of the preset options is used in the customer network, the ToS value can also be set directly and manually. The set value is set to decimal 0-63 and transferred to the upper 6 bits of the ToS byte (e.g., 41 = 101-001-00 = 0xA4).

Table of Possible Priority Classes

Priority class	ToS value, binary	ToS value, hexadecimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60

Priority class	ToS value, binary	ToS value, hexadecimal
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Manual entry	xxx-xxx-00	0-63 (decimal)

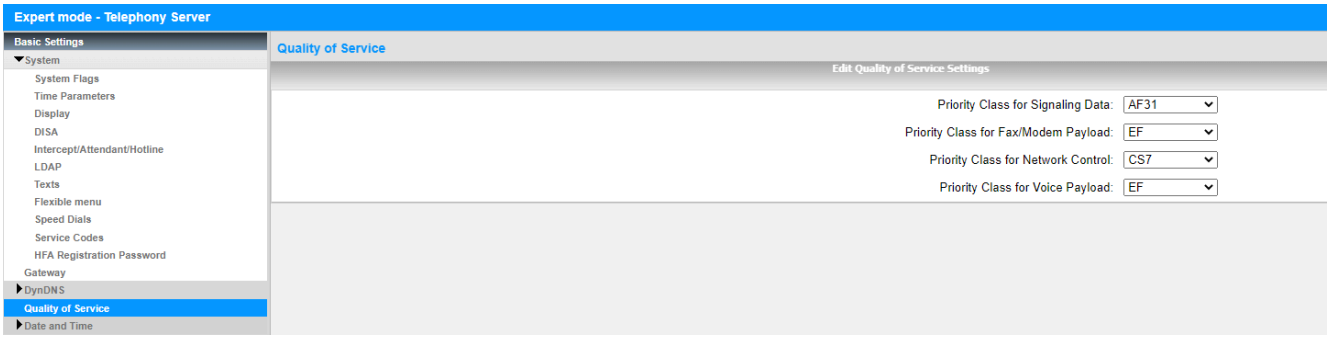
11.2.3.1 How to Configure Quality of Service (QoS)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Quality of Service**.



4) Select the priority class you want in the **Priority Class for Signaling Data** drop-down list.
5) Select the priority class you want in the **Priority Class for Fax/Modem Payload** drop-down list.
6) Select the priority class you want in the **Priority Class for Network Control** drop-down list.
7) Select the priority class you want in the **Priority Class for Voice Payload** drop-down list.
8) Click on **Apply**, followed by **OK**.

11.3 IP Stations

IP stations are connected to the communication system via the LAN. An IP station is generally a LAN or WLAN phone.

The following IP protocols are supported:

- Vendor-specific communication system protocol

  The communication system uses CorNet-IP (CorNet Internet Protocol) for LAN telephony within the internal network. CorNet-IP, which was developed

on the basis of H.323, supports all telephone features of the communication system.

- SIP (Session Initiation Protocol)

  SIP is usually used in Internet telephony but is not restricted to it. It can also be used for telephony in the internal network, for example. However, SIP does not support all telephony features associated with the communication system.

The following types of IP stations exist:

- **System Client**: A system client is an IP station that can use all the features of the communication system via CorNet-IP. This can be an IP system phone such as an OpenStage 60 HFA, for instance, or a PC with CTI software such as OpenScape Personal Edition.
- **SIP client**: A SIP client is an IP station that uses the SIP protocol. It can access only limited functionality of the communication system via SIP. A SIP client is a SIP phone such as the OpenStage 15 S, for example.
- **Deskshare User**: A Deskshare User is an IP user who can log in at another IP system telephone (mobile login) and then use this phone as his or her own phone (including the call number).
- **RAS User**: A RAS user (Remote Access Service user) is granted access to the IP network via the ISDN connection. This allows the communication system to be maintained remotely.

For each connected IP station, an "IP User" station license is required.

Two IP stations are reserved for the Online User and for remote access via ISDN. These IP stations do not require a station license. If one or several of these three reserved IP stations are not required, these stations can be converted to normal IP stations in Expert mode. However, station licenses are then required for these IP stations.

Configuring IP Stations

The following configurations can be performed for an IP station:

- Configuration of standard parameters with the **IP Telephones** wizard (see How to Configure IP Stations).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see Station>Station>IPClients).

OpenScape Desk Phone IP system phones are supplied with the SIP software by default. As soon as an OpenScape Desk Phone IP system phone is configured in the WBM as a **System Client**, the HFA software stored in the communication system is automatically loaded onto the IP system phone.

11.4 SIP Stations

SIP stations are IP stations that use the Session Initiation Protocol (SIP) for communication. SIP stations can use this protocol to access a limited number of the communication system's functions. SIP stations, like IP stations, are connected to the communication system over the LAN.

A SIP station is a WLAN phone or a LAN phone such as the OpenStage 15 S, for example.

For each connected SIP station, an "IP User" station license is required.

SIP Authentication

In order to ensure the security of the internal network, it is important that SIP subscribers are authenticated at the communication system with the values described below. These values must be configured in the WBM of the communication system for each SIP subscriber and also at every SIP phone itself. To protect against SIP attacks, authentication is strongly recommended!

- Password

  Password for authentication: assigned freely; at least 8 characters up to a maximum of 20 characters. The password should contain at least one uppercase letter, one lowercase letter, one digit and one special character. A separate password should be assigned for each SIP subscriber.
- SIP User ID / Username

  User name for authentication: preassigned; can be changed if required, maximum 20 characters. Each SIP subscriber has a different preassigned SIP User ID.
- Realm

  Zone or domain for authentication: assigned freely; can be changed if required, max. 20 characters. The realm for all SIP subscribers is preassigned with the same value. It can be changed as required, e.g., in the host name or domain name of the communication system.

Configuration of SIP Stations in the Communication System

The following configurations can be performed in the WBM of the communication system for an IP station:

- Configuration of standard parameters with the **IP Telephones** wizard (see How to Configure SIP Stations).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see Station>Station>IPClients).

Configuration of the SIP phone

The data used to authenticate a SIP subscriber at the communication system must be additionally entered directly at the SIP phone.

Configuration of authentication data at the SIP phone (see Configuring the Authentication Data at the SIP Phone).

Features that can be used with SIP Telephones

The following features can be used with SIP telephones:

- Incoming and outgoing calls with display of call number and name
- Hold, Toggle/Connect, Consultation
- Call transfer (screened/unscreened)
- Take Call
- Immediate call forwarding, on busy and after timeout
- Three-party conference
- Call lists, message waiting indicator
- Ringer cutoff at phone, reject call, call forwarding
- Call waiting
- Membership in groups (without display of the group number)
- Different calls for internal, external and recall

- Mailbox LED - Message Waiting Indication
- DTMF dialing, e.g., for the operation of voicemail boxes
- Use of the UC clients
- Automatic software updates (when using the DLI)

NOTICE: Deployment with a multichannel Contact Center has not been released (e.g. transfer to UCD groups).

Depending on the telephone, there may be some restrictions on the available functions; see the wiki at:

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

The following features, which are activated using service codes with * or #, can be used with SIP phones:

- Reset all services: #0
- Call forwarding: *1xf (x = 1 - all, 2 - internal, 3 - external) (f = forwarding number)
- Call forwarding off: #1
- Leave/Rejoin hunt group: #85g/*85g (g = group number, optional - needed when in multiple groups)
- Suppress/Enable Calling ID (CLIR): *86/#86
- Speed dial: * 7nnnn (nnnn = speed dial number)
- Door opener: *61

INFO: It is recommended to use * or # substitution codes for best compatibility with 3rd party SIP devices. The SIP user has to send the full service code sequence as a block-dial.

INFO: Unlike HFA devices, there is no user interaction or guidance for service code sequences on SIP devices. The full service code sequence has to be dialed at once.

Features that can be used with SIP Telephones and myPortal/myAttendant

SIP phones to be used with myPortal and myAttendant must meet the following requirements:

- 3PCC as per RFC 3725 is supported.
- The "call waiting" feature is supported.
- The local Do Not Disturb is disabled.

The full functionality of the features depends on the SIP phone used and cannot be guaranteed. A successful test of the features listed below was performed with the OpenStage SIP telephones.

Connection-/call-oriented features:

- Making Call
- Redirect call
- Take Call
- Resume call
- Application-controlled conference

- Place call on hold
- Alternate (Toggle/Connect)
- Consultation
- Disconnect
- Transfer

Phone-oriented features:

- Do Not Disturb
- Call forwarding

11.5 UP0 stations

A UP0 station uses a $U_{P0/E}$ line to transmit digital signals. UP0 stations are connected to the communication system via UP0 interfaces and are system telephones such as an OpenStage 60T, for example. UP0 stations can therefore use the complete functional scope of the communication system.

The following connectivity options are available for UP0 stations:

- OpenScape Business X1

  To the $U_{P0/E}$ interfaces on the mainboard.
- OpenScape Business X3/X5

  To the $U_{P0/E}$ interfaces on the mainboard or, if several UP0 stations are involved, to an additionally inserted $U_{P0/E}$ board.
- OpenScape Business X8

  To additionally inserted $U_{P0/E}$ boards.
- OpenScape Business S

  No connection possible.

For each connected UP0 station, a "TDM User" station license is required. Even system telephones that are connected in slave mode require a station license.

Configuring the UP0 Stations

The following configurations can be performed for a UP0 station:

- Configuration of standard parameters with the **UP0 Devices** wizard (see How to Configure UP0 Stations).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see Station>Station>UP0Stations).

11.6 DECT stations

A DECT station uses a Cordless base station to transmit digital signals. A DECT station is a DECT telephone.

The following connection options are available for DECT stations:

- OpenScape Business X1W/X1R/X3W/X3R/X5R

  Cordless base station to a $U_{P0/E}$ interface of the mainboard.

- OpenScape Business X8

  Cordless base station to one or more SLMUC boards.
- OpenScape Business S

  DECT IP base station on the LAN

The connection of a Cordless base station is called the integrated Cordless solution. This means that almost all functions of the communication system are available.

The integration of an IP DECT base station in the internal network is called Cordless IP. Since only the SIP protocol can be used in this case, not all communication system features are available.

For each connected DECT station, a "TDM User" station license is required.

For the description and configuration of the integrated Cordless solution, see Integrated Cordless Solution.

Configuring DECT Stations

The following configurations can be performed for a DECT station:

- Configuration of standard parameters with the **DECT Devices** wizard (see How to Configure DECT Stations).
- Configuration of all parameters (standard and advanced parameters in Expert mode (see Station>Station>DECTStations>DECT Stations).

DECT IP stations are configured as normal SIP stations.

11.7 Mitel SIP DECT stations

The following connection options are available for Mitel SIP DECT stations:

- OpenScape Business S systems
- OpenScape Business V3 hardware (OCCe)

Provisioning Mitel SIP DECT RFP Stations

The process includes the following general steps:

1) Configure the DHCP with a static IP address for the OMM base station.
2) The base station will get an IP address and start the OMM application.
3) Configure the base station through its web interface.
4) The base station will automatically fetch the configuration files from OpenScape Business.
5) When a handset logs in, the base station will also fetch the user's configuration file and set-up the handset.

Configuring Mitel SIP DECT Stations via WBM

The following configuration steps must be performed:

1) Enable DHCP server and provide a static IP address for the OMM base station (see Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Static IP Addresses).
2) Configuration of standard parameters with the Mitel SIP DECT Devices wizard (see How to Configure Mitel SIP DECT Stations).

3) Configuration SIP stations and its parameters via the Expert mode (see How to Configure SIP Stations via Expert Mode).

11.8 ISDN Stations

An ISDN station uses the $_0$ bus for transmitting digital signals and is therefore often referred to an S_0 station The ISDN station is connected to the communication system via the S_0 interfaces

The following connection options are available for an S_0 station:

- OpenScape Business X1

  To an S_0 interface of the mainboard.
- OpenScape Business X3/X5

  To an S_0 interface of the mainboard or to an S_0 board.
- OpenScape Business X8

  To one or more S_0 boards.
- OpenScape Business S

  To additionally required gateways or adapters

The following ISDN stations can be connected:

- ISDN phone
- Fax Group 4
- ISDN modem
- PC with ISDN card

The following types of ISDN stations can be defined:

- Default: for ISDN phone, Fax Group 4, ISDN modem or PC with ISDN card
- Fax: prerequisites for setting up the "Info from Fax/Answering Machine" key. If a PC with an ISDN card and Fax software is attached to the S_0 bus and assigned the type "Fax", for example, then an "Info from Fax/Answering Machine" key could be set up on every device. When this key lights up, this indicates that a fax has been received.
- Answering machine: prerequisites for picking up a call when the answering machine has already accepted it If a Gigaset ISDN phone with an answering machine is connected and assigned the type "Answering Machine", for example, a call that has already been accepted by the answering machine can be picked up at any terminal. To do this, the terminal must be programmed with the internal call number of the Gigaset.

For each connected ISDN station, a "TDM User" station license is required.

Connecting ISDN Stations to the S_0 Port

To be able to connect an ISDN station to the communication system, you must configure at least one of the S_0 ports that are used for the ISDN subscriber line or the ISDN point-to-point connection as an internal S_0 bus (S_0 EURO bus).

NOTICE: If there is more than one ISDN station connected to an S_0 port (up to 8 ISDN stations are possible) in an ISDN point-to-multipoint connection, each individual ISDN station must be

assigned to a unique MSN. This assignment must be made in the configuration menu of the ISDN station.

Configuring ISDN stations

The following configurations can be performed for an ISDN station:

- Configuration of standard parameters with the **ISDN Devices** wizard (see How to Configure ISDN Stations).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see Station>Station>ISDNStations).

Allowing only Configured Numbers for MSNs

The administrator can specify that further MSNs at an S0 bus may only be configured for call numbers that already exist there. This prevents subscribers from adding an MSN without authorization through an outgoing seizure of the S0 bus with a further MSN. Without this restriction, the communication system would normally assign a free internal call number to the S0 bus for that MSN.

Terminal Portability

The communication system supports Terminal Portability (TP), that is, it lets you park a call on the S_0 bus, unplug the terminal, and plug it back in at a new location to resume the call. The parked station receives a message indicating that the user is porting. Three minutes are available for the entire operation.

The feature is not supported for services such as telefax, teletex or data transfer.

11.8.1 How to Configure the S_0 Interface for ISDN Stations

You can use the **CO Trunk ISDN / Analog / ITSP** wizard to configure one or more S_0 ports so that ISDN phones can be connected to them.

Prerequisites

One or more free S_0 interfaces are available.

You are logged on to the WBM with the **Advanced** profile.

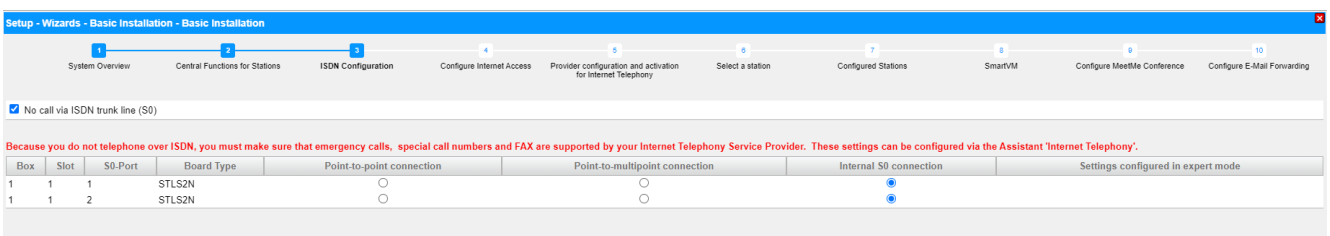
Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Central Telephony**.

3) Click **Edit** in the **CO Trunk ISDN / Analog / ITSP** wizard.

4) Click on **OK & Next**. The existing S_0 interfaces (S_0 ports) are displayed.



5) Do not alter the setting for the check box **No call via ISDN trunk line (S0)**.

6) Activate the Internal S0 connection radio button for the desired S**0** ports.

NOTICE: These S_0 ports can no longer be used for ISDN trunk access.

---

7) Keep clicking **OK & Next** until you receive a message that the editing of the feature has been completed.
8) Click on **Finish**.

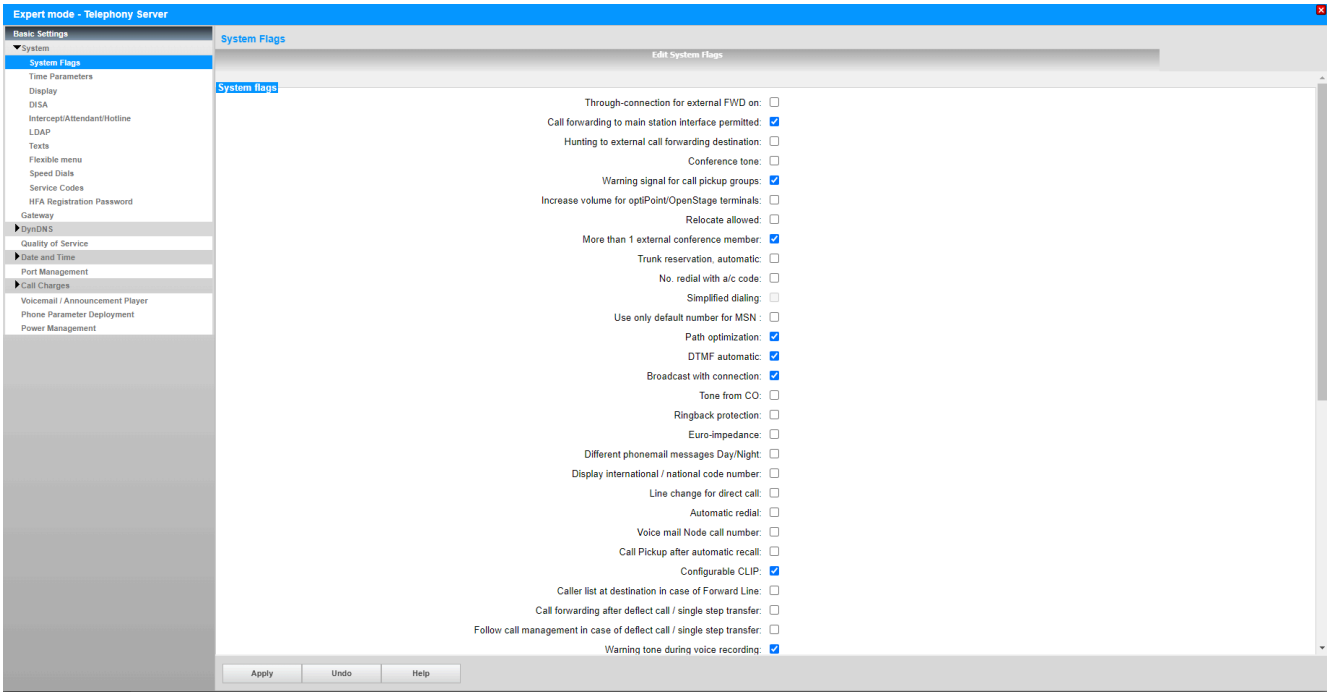
11.8.2 How to Allow only Configured Numbers for MSNs

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **System Flags**.



4) If you want to allow only configured numbers for MSNs, enable the check box **Use only default number for MSN**.
5) If you do not want to allow only configured numbers for MSNs, clear the check box **Use only default number for MSN**.
6) Click on **Apply** followed by **OK**.

11.9 Analog Stations

An analog station uses a two-core analog cable to transmit analog signals. The communication system connects the analog station via the analog ports.

The following connectivity options are available for analog stations:

- OpenScape Business X1

  To an analog interface of the mainboard.
- OpenScape Business X3/X5

  To an analog interface of the mainboard or to an analog board.
- OpenScape Business X8

  To one or more analog boards.
- OpenScape Business S

  To additionally required gateways or adapters

The following analog stations can be connected:

- Analog telephone
- Analog Fax (Group 3)
- Answering Machine
- Modem, 9600 bps or higher
- Entrance Telephone (Door Opener)
- Loudspeaker

The following types of analog stations can be defined:

- Standard: for analog phone, Group 3 fax, answering machine or loudspeakers
- Fax: prerequisites for setting up the "Info from Fax/Answering Machine" key. If a Fax Group 3 device is connected and assigned the type "Fax", for example, then an "Info from Fax/Answering Machine" key could be set up on every device. When this key lights up, this indicates that a fax has been received.
- Answering machine: prerequisites for picking up a call when the answering machine has already accepted it If a Gigaset phone with an answering machine is connected and assigned the type "Answering Machine", for example, a call that has already been accepted by the answering machine can be picked up at any terminal. To do this, the terminal must be programmed with the internal call number of the Gigaset.
- Modem: Analog modems with a fixed speed of 56 kbps or higher are not supported, since speeds of 56 kbps or higher cannot be processed.

For each connected analog station, a "TDM User" station license is required.

Availability of an Analog Fax Device in the System with Previous Fax Number

Since it is not possible to forward an analog fax device to a fax number in the system, the following workaround exists: The previous fax number is configured in the system and receives the incoming fax messages. For the analog fax device, a port is configured with the previous number as the CLIP. The Configurable CLIP check box must be selected for this purpose. Outbound fax messages show the previous number as the sender; internal recipients see the internal number of the fax machine.

Configuring Analog Stations

The following configurations can be performed for an analog station:

- Configuration of standard parameters with the **Analog Devices** wizard (see How to Configure Analog Stations).
- Configuration of all parameters (standard and advanced parameters via Expert mode (see Station>Station>AnalogStations).

11.10 Virtual Stations

Virtual stations behave like real stations, but have no physical telephones assigned to them.

Virtual stations are required for mobile phone integration and call forwarding no answer (CFNA), for example. These stations must be configured like real stations so that they can be used for the signaling of calls, for example.

Configuring Virtual Stations

The parameters associated with a virtual station are configured in Expert mode (see Station>Station>VirtualStations).

11.11 Key programming

Every system phone comes with a certain number of function keys. A number of these function keys are programmed by default with functions. You can modify this default setting and program the remaining function keys that were not preprogrammed.

The individual keys can be programmed as follows:

- Key programming via WBM

  The keys on connected system telephones can be programmed in the WBM via the **Key Programming** wizard.

  This wizard can also be used to program a key assignment for a subscriber even though no system telephone has been connected for that subscriber.
- Key programming via the UC clients

  Users of the UC clients **myPortal for Desktop**, **myPortal for Outlook** and **myAttendant** can also program the keys on their system telephone via these UC clients (see the respective User Guides for the UC clients).
- Key programming directly at the system telephone

  System phones with display allow you to program certain function keys directly at the phone.

Programming Function Keys on Different Levels

The function keys of the system telephones can be programmed twice, that is, on the first and second levels. You can program all available functions on the first level. You can program external phone numbers on the second level. The Shift key must be programmed on the system phone before you can use the second level. The function key LEDs are always assigned to the first level.

NOTICE: In case of a **user it is not possible to copy key programming as the automatic key assignment feature is

MULAP specific and should not be copied at any station. The prefix ** should be removed manually from these users in order the key copy to be enabled.

11.11.1 How to Program the Function Keys on the System Phones

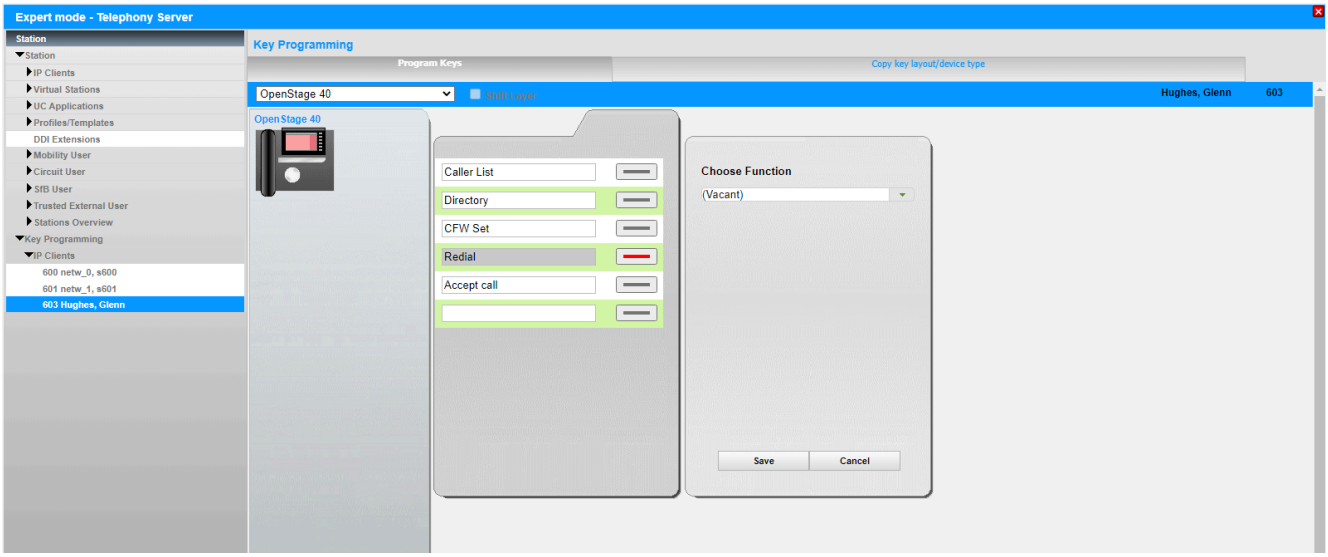
You can use the **Key Programming** wizard to configure the function keys on the system phones.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click **Edit** to start the **Key Programming** wizard. A list of all stations is displayed.
4) Click **Edit** in the row containing the station you want.
5) Assign the system phone to the station:
   - If a system telephone is already connected for the station, you will be presented with a simplified display of the system telephone.
   - If no system telephone is connected for the station as yet, select the system telephone to be connected from the drop-down list. You will then be presented with a simplified display of the system telephone.
6) Click in the simplified display of the system telephone on the desired key field. The function keys of the selected key field will be displayed with the currently assigned functions.



7) Assign functions to the function keys:

a) Click on the key symbol for the function key to be assigned. A drop-down list with the available functions appears.

b) Select one of the offered choices **Select Function** drop-down list.

c) Some functions require additional information. Select this as needed or enter the required data.

d) Click **Save**.

e) If required, edit the function key label in the **Change predefined label** field.

NOTICE: If you have a system telephone with automatic key labeling (such as an OpenStage 60 HFA, for example), this text will appear in the display of the system telephone.

---

f) Click **Save**.

g) If you want to assign functions to further function keys, repeat step 7.

8) If you programmed a function key as the **Shift Key**, select the **Shift Key** check box. Program the second level of the function keys with the external call numbers as described below under step 7.

9) Click **Save Keypad**.

10) If you want to apply the key assignment just completed to several or all system telephones, enable the check box for the desired system phones and then click on **Apply**, **OK** and **OK & Next**.

11) If you want to apply the key assignment just completed to only the selected system telephone, first click on **Deselect all stations** to be on the safe side and then on **OK & Next**.

12) Click **Next** followed by **Finish**.

11.12 Station Profiles

The values and properties of subscribers are stored in profiles. One or more members can be assigned to a profile. The same values and properties then apply to all members of that profile.

Station profiles can be assigned to subscribers with system telephones. Up to 20 station profiles can be created. The station profiles can be exported or imported individually or collectively. The files are of type `xml`.

Every subscriber can be a member of exactly one profile. If the values and properties of a station that is a member of a profile are changed directly, i.e., not through the profile, the station is deleted from the profile.

11.13 Configuring Stations

You can define specific values (for example, phone number, name, and DID number) and properties (for example, type of call signaling) for the station.

Station configuration is split into standard configuration and advanced configuration. The default settings can be configured using wizards with the **Advanced** profile. The Advanced settings can only be configured in Expert mode with the **Expert** profile.

The default settings can be conveniently edited in a list for all stations of a station type (e.g., IP stations or analog stations). Additional settings (such as call signaling or the station flags, for example) can be changed individually for each subscriber.

Virtual stations are configured entirely in Expert mode (both the standard and the advanced settings).

Although the **Basic** profile cannot be used to configure stations, it can be used to edit the names of stations.

A dial plan (also called a numbering plan) should be available for the stations connected to the communication system. The station numbers, names and DID numbers of all configured subscribers can be displayed in Expert mode via **Stations** > **DDI Extensions**.

DID numbers which are not provided by the service provider and which are not used in the system should be deleted; otherwise, there may be conflicts with MSN or Internet telephony phone numbers. DID numbers that are provided by an Internet Telephony Service Provider (ITSP) must be assigned to the individual stations when configuring the ITSP (see Configuring an ITSP).

IMPORTANT: Whenever the phone number of a station is changed, the Smart VM (Voicemail) configured for that station is automatically reset. All personal voice messages, greetings and announcements are lost, and the password is reset.

Default Settings

The default settings should be verified for every station and adapted if required.

- **Station Number, Name, DID Number**

  Every station is assigned a station number by default (such as 101). The station can be reached internally under this call number. In system phones, this phone number appears both on the actual display and the communication partner's display. If a station number other than the actual station number is to be displayed at the external station called, this number can be defined here.

  You can also assign a DID number to each station. The station can be accessed directly from an external location with the DID number. The station can be reached internally via the call number 101, for example, and externally via the DID number `3654321` (MSN in a point-to-multipoint connection) or `<PABX number>-101` (in a point-to-point connection). In the case of a point-to-point connection, you can configure whether the internal phone number should be automatically entered as a DID number during initial installation. The DID number may also differ from the phone number. If you are using Internet telephony, you can also define a DID number that can be used to reach the station via Internet telephony. This phone number is made available by the Internet Telephony Service Provider.

  You can also assign a name to each station. This name appears on the communication partner's display (system phones only).

  If a dial plan exists, the phone numbers, DID numbers, and names of the subscribers should be adjusted based on the dial plan.

- **Type**

  The station type can be selected for every station. For example, an IP station could have a station type of **System Client** or **SIP Client**; an analog station may be an analog phone or an analog fax machine, and an ISDN station could be an ISDN phone or ISDN fax.
- **Fax call number; Fax DID number**

  If the a fax box is to be set up for a subscriber (which can be used with the UC clients myPortal for Desktop or myPortal for Outlook, for example), assign a fax call number (for receiving internal faxes) and a fax DID number (for receiving external faxes).
- **Classes of Service**

  A station can be assigned one out of 15 possible classes of service. This determines whether a station may accept and make external calls, for example, or which numbers may be dialed by the station and which are not allowed (see Classes of Service (Toll Restriction)).
- **Call pickup group**

  Every station can be assigned to a call pickup group.
- **Language, call signaling**

  The language used for the menu controls of the attached system telephones can be set.

  The ring tone for an internal or external call can be selected.
- **Voicemail box (only with UC Smart)**

  With the UC solution UC Smart, you can set up a voicemail box for each subscriber and choose between different greetings. For more detailed information on the voicemail box, see Voicemail Box (SmartVM)

  With the UC solution UC Suite, a voicemail box is assigned automatically to each subscriber. Consequently, there are no voicemail box settings in this case.
- **Station flags**

  The station flags of each subscriber can be changed. For a description of the station flags, see Station>Station>StationParameters.

Advanced Settings

You can configure all settings for all types of stations in Expert mode. The advanced settings can be left unaltered for default operation and only have to be changed if required. For information on the advanced settings, see Station .

Related concepts

Classes of Service (Toll Restriction) on page 721
Multilingual Text Output on page 1172

11.13.1 How to Configure IP Stations

You can use the **IP Telephones** wizard to configure the IP stations (LAN phones and WLAN phones).

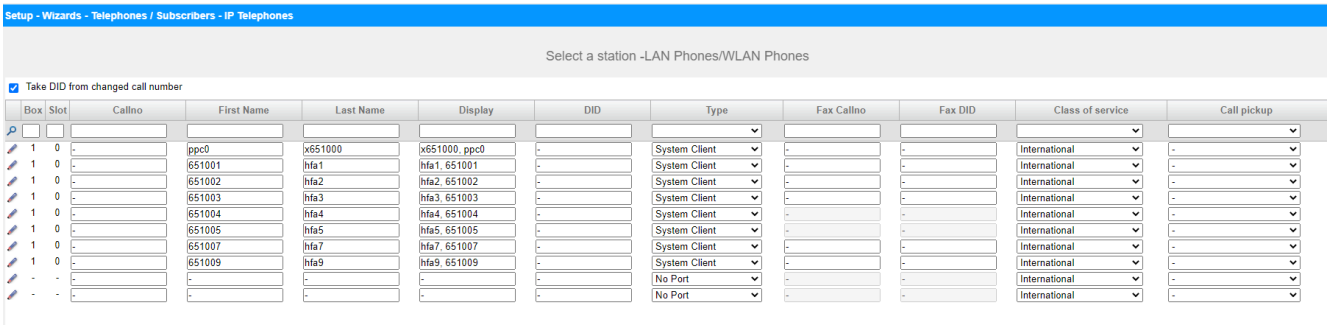
Prerequisites

A functional wireless LAN network is needed to operate WLAN phones.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click on **Edit** to start the **IP Telephones** wizard. A list of all IP stations appears.



4) If you want the internal call number to be automatically assigned to the station as the direct inward dialing number, activate the radio button **Take DID from changed call number**.
5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:
   - Only for a point-to-point connection:

     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.
6) If you want an Internet telephony phone number to be assigned to the station as the direct inward dialing number, leave the radio button **Take DID from changed call number** unselected, and select the Internet Telephony Service Provider from the list next to the radio button instead. Then select the Internet Telephony phone number from the **DID** drop-down list in the row of the desired station.
7) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.
8) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

9) Select the type of IP station (e.g., **System Client** or **DeskShare User**) from the **Type** drop-down list in the row of the desired station).

10) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

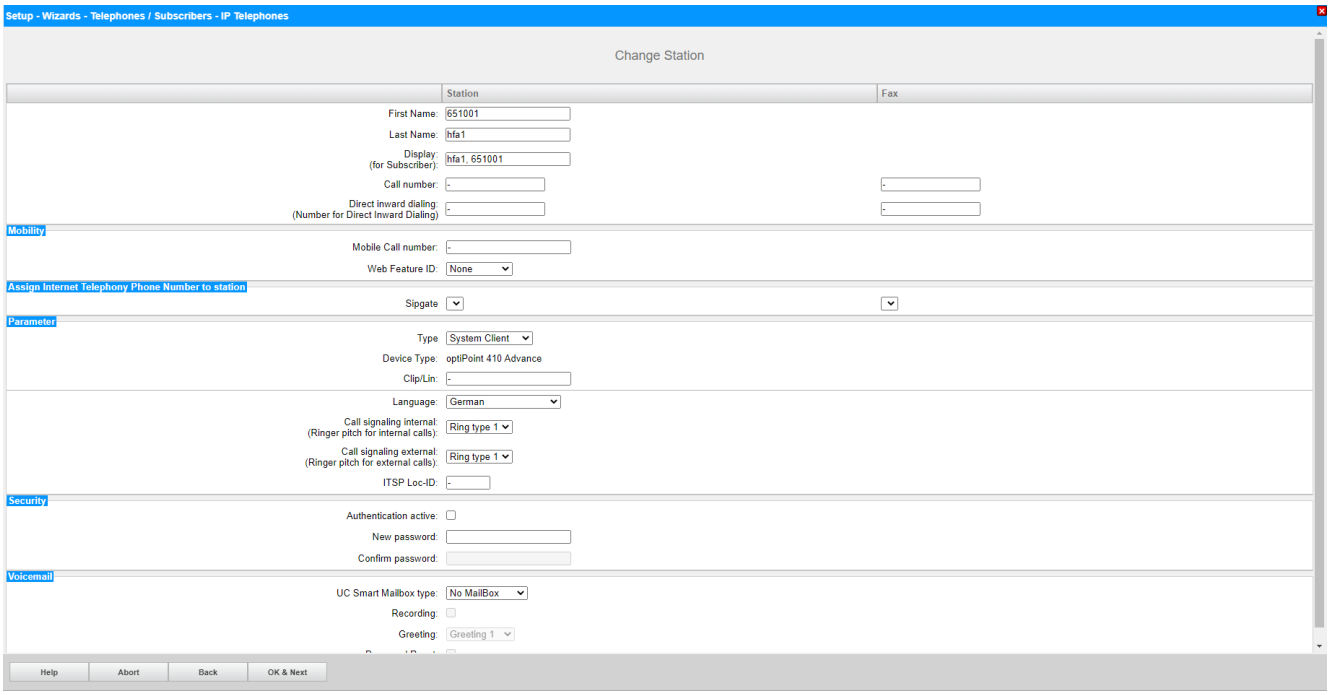
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax DID** field in the row of the desired subscriber.

11) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

12) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

13) Make any further settings if required:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) Assign one **Mobile Call number** and select the **Web Feature ID** from the drop-down list in the **Mobility** area.

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is

formatted and sent as the Calling Party Number for the external call.

d) Select the language for the menu controls on the phone from the **Language** drop-down list.
e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).
f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).
g) In the **ITSP Loc-ID** field, enter the index number of the ITSP Location ID.
h) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
i) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
j) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.
k) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

l) If the station is connected to the internet, Authentication MUST be activated and you MUST enter strong passwords for all IP stations. Check the **Authentication active** flag list and complete the **New password** and **Confirm password** fields.
m) Click on **OK & Next**.
n) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.
o) Click on **OK & Next**.

14) If you want to configure another station, repeat steps 5 through 13.
15) Click on **OK & Next**. A list of all configured IP stations appears. If required, you can print the list of IP stations with **Print**.
16) Click on **OK & Next** followed by **Finish**.

11.13.2 How to Configure SIP Stations

You can use the **IP Telephones** wizard to configure the SIP stations (LAN phones and WLAN phones).

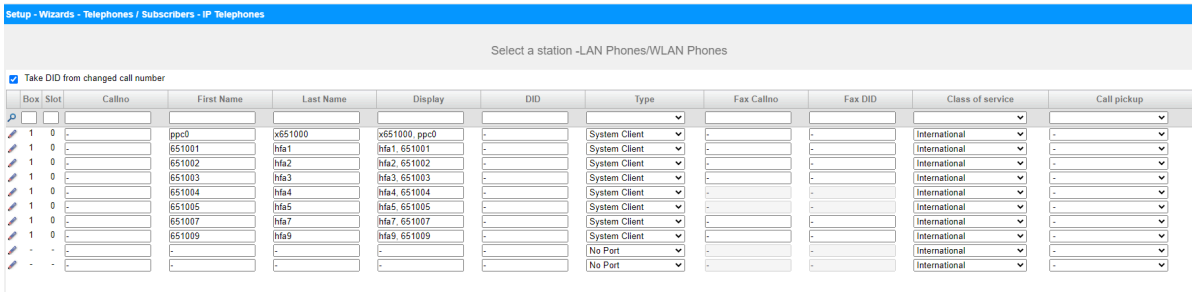
Prerequisites

A functional wireless LAN network is needed to operate WLAN phones.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click on **Edit** to start the **IP Telephones** wizard. A list of all IP stations appears. This list also includes all SIP stations.



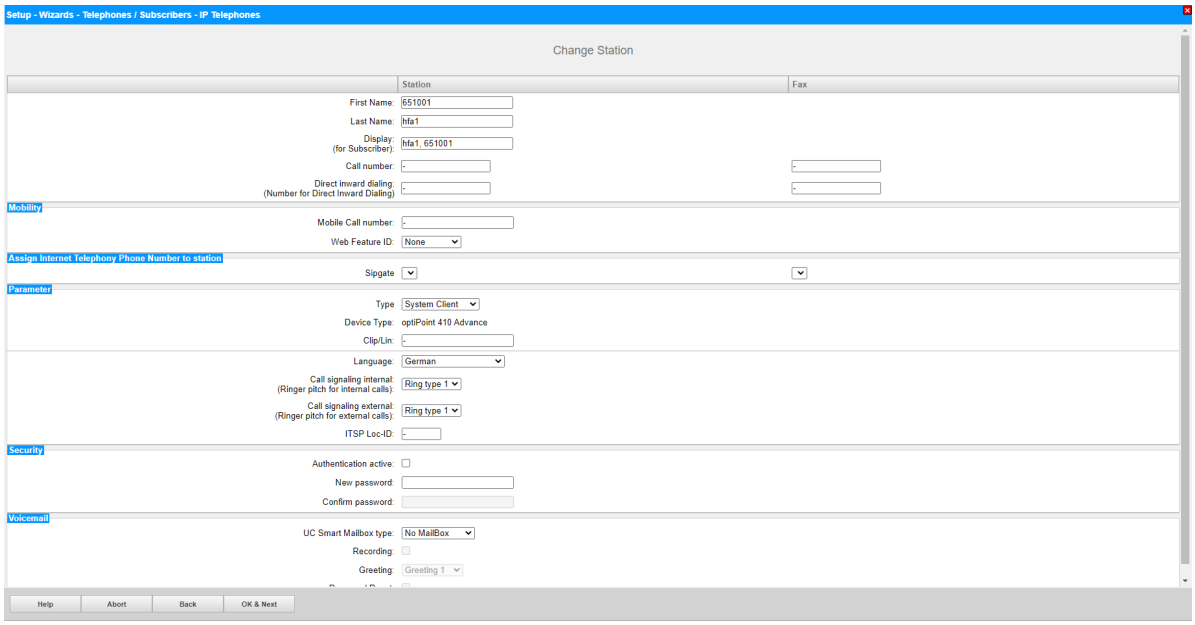
4) If you want the internal call number to be automatically assigned to the station as the direct inward dialing number, activate the radio button **Take DID from changed call number**.
5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:
   - Only for a point-to-point connection:

     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.
6) If you want an Internet telephony phone number to be assigned to the station as the direct inward dialing number, leave the radio button **Take DID from changed call number** unselected, and select the Internet Telephony Service Provider from the list next to the radio button instead. Then select the Internet Telephony phone number from the **DID** drop-down list in the row of the desired station.
7) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.
8) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.
9) Select **SIP Client** from the **Type** drop-down list in the row of the desired station.

10) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:
   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.
   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax DID** field in the row of the desired subscriber.
11) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.
12) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.
13) Configure the data for SIP:
   a) Click in the row of the desired station on the pencil icon **Edit**.



   b) In the **Security** area, enter the password for the authentication of the SIP station in the **Password** and **Confirm password** fields.
   c) Assign a user name of your choice for the authentication of SIP station, e.g., SIP-120, in the **SIP User ID / Username** field.
   d) Under **Realm**, assign a name of your choice for the associated zone, e.g., OSBIZ-SIP. This value should be the same for all SIP stations.

> **NOTICE:** The values defined here for the password, SIP user ID and realm must also be entered at the SIP phone.

14) Make any further settings if required:
   a) If this SIP phone is to be operated in conjunction with a dual-mode mobile phone, enter the dialout prefix followed by the telephone number of the mobile phone (e.g., `0016012345678`) in the **Mobility** area under **Mobile phone number**. In addition, select this SIP client from the **Web Feature ID** drop-down list. (see Dual-Mode Telephony).

b) Assign one DID number each for Internet telephony to the station and, if desired, to its fax box in the **Direct inward dialing for Internet Telephony** area. To do this, select the DID numbers from the drop-down lists of the desired ITSPs. For every active ITSP, you will be presented with one drop-down list for the station and one drop-down list for its fax box.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

d) Select the language for the menu controls on the phone from the **Language** drop-down list.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.

h) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.

i) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.

j) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

---

k) Click on **OK & Next**.

l) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

m) Click on **OK & Next**.

15) If you want to configure another station, repeat steps 5 through 14.

16) Click on **OK & Next**. A list of all configured IP stations appears. If required, you can print the list of IP stations with **Print**.

17) Click on **OK & Next** followed by **Finish**.

11.13.3 How to Configure UP0 Stations

You can use the **UP0 Devices** wizard to configure the UP0 stations.

Prerequisites

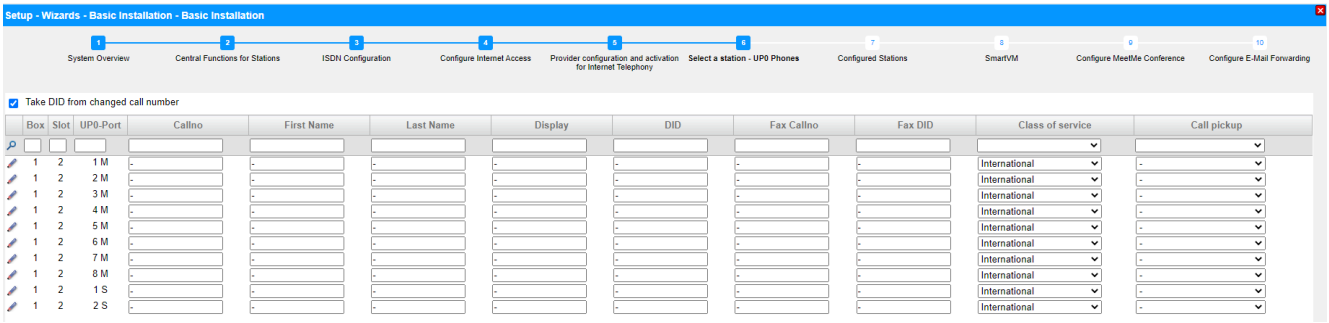
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.

3) Click on **Edit** to start the **UP0 Devices** wizard. A list of all UP0 stations appears.



4) If you want the internal call number to be automatically assigned to the station as the direct inward dialing number, activate the radio button **Take DID from changed call number**.

5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

- Only for a point-to-point connection:

  Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
- Only for a point-to-multipoint connection:

  Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
- For point-to-point and point-to-multipoint connections:

  Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

6) If you want an Internet telephony phone number to be assigned to the station as the direct inward dialing number, leave the radio button **Take DID**

from changed call number unselected, and select the Internet Telephony Service Provider from the list next to the radio button instead. Then select the Internet Telephony phone number from the **DID** drop-down list in the row of the desired station.

7) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

8) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

9) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

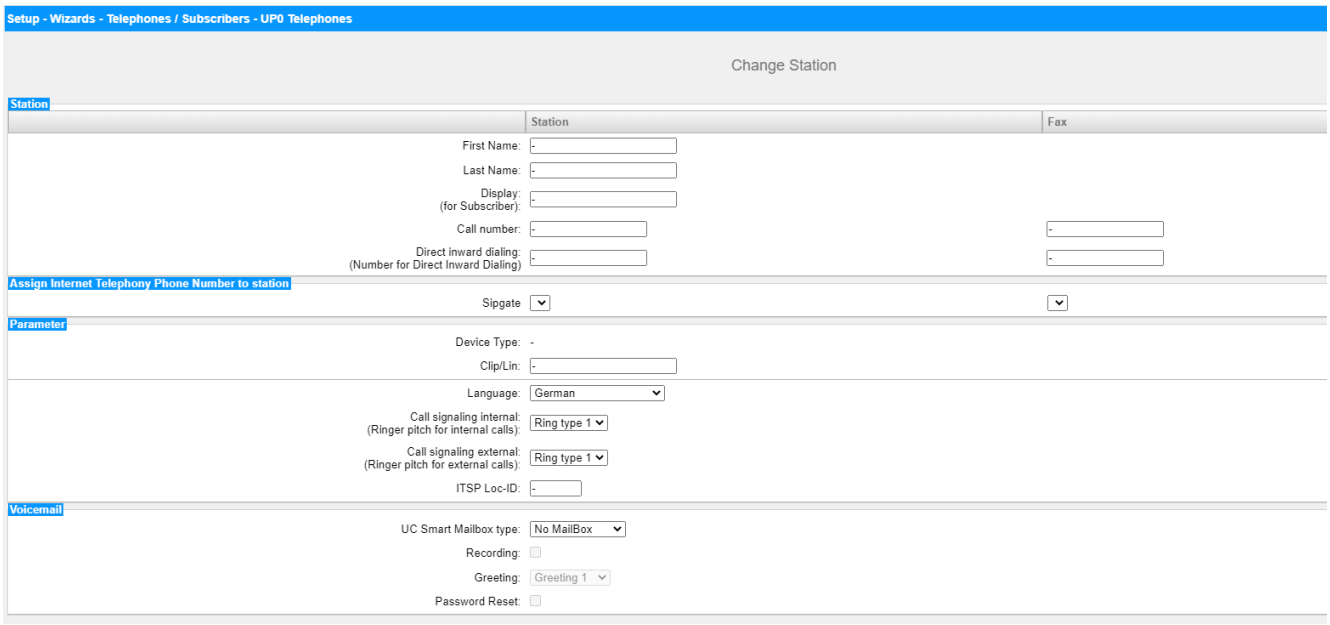
b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax DID** field in the row of the desired subscriber.

10) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

11) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

12) Make any further settings if required:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is formatted and sent as the Calling Party Number for the external call.

---

d) Select the language for the menu controls on the phone from the **Language** drop-down list.

e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal

stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

g) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.

h) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.

i) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.

j) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

---

k) Click on **OK & Next**.

l) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.

m) Click on **OK & Next**.

13) If you want to configure another station, repeat steps 5 through 12.

14) Click on **OK & Next**. A list of all configured UP0 stations appears. If required, you can print the list of UP0 stations with **Print**.

15) Click on **OK & Next** followed by **Finish**.

11.13.4 How to Configure DECT Stations

You can use the **DECT Devices** wizard to configure the DECT stations (DECT phones).

Prerequisites

A base station is connected to a UP0 interface or to an installed SLC board.

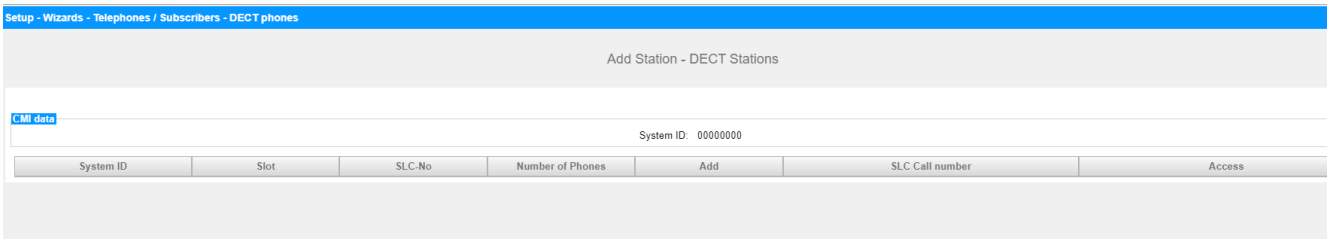
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.

3) Click on **Edit** to start the **DECT Phones** wizard. A list of all DECT stations appears.



4) If you want the internal call number to be automatically assigned to the station as the direct inward dialing number, activate the radio button **Take DID from changed call number**.

5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:

   - Only for a point-to-point connection:

     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

6) If you want an Internet telephony phone number to be assigned to the station as the direct inward dialing number, leave the radio button **Take DID from changed call number** unselected, and select the Internet Telephony Service Provider from the list next to the radio button instead. Then select the Internet Telephony phone number from the **DID** drop-down list in the row of the desired station.

7) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

8) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

9) If you want to set up a fax box for the subscriber (which can be used with the UC clients **myPortal for Desktop** or **myPortal for Outlook**, for example), proceed as follows:

   a) In the row of the desired station, in the **Fax No.** field, enter the desired internal fax number at which the user can receive internal fax messages.

   b) If you want to configure a DID number for the fax box, enter the desired external fax number under which the subscriber can receive external fax messages in the **Fax DID** field in the row of the desired subscriber.

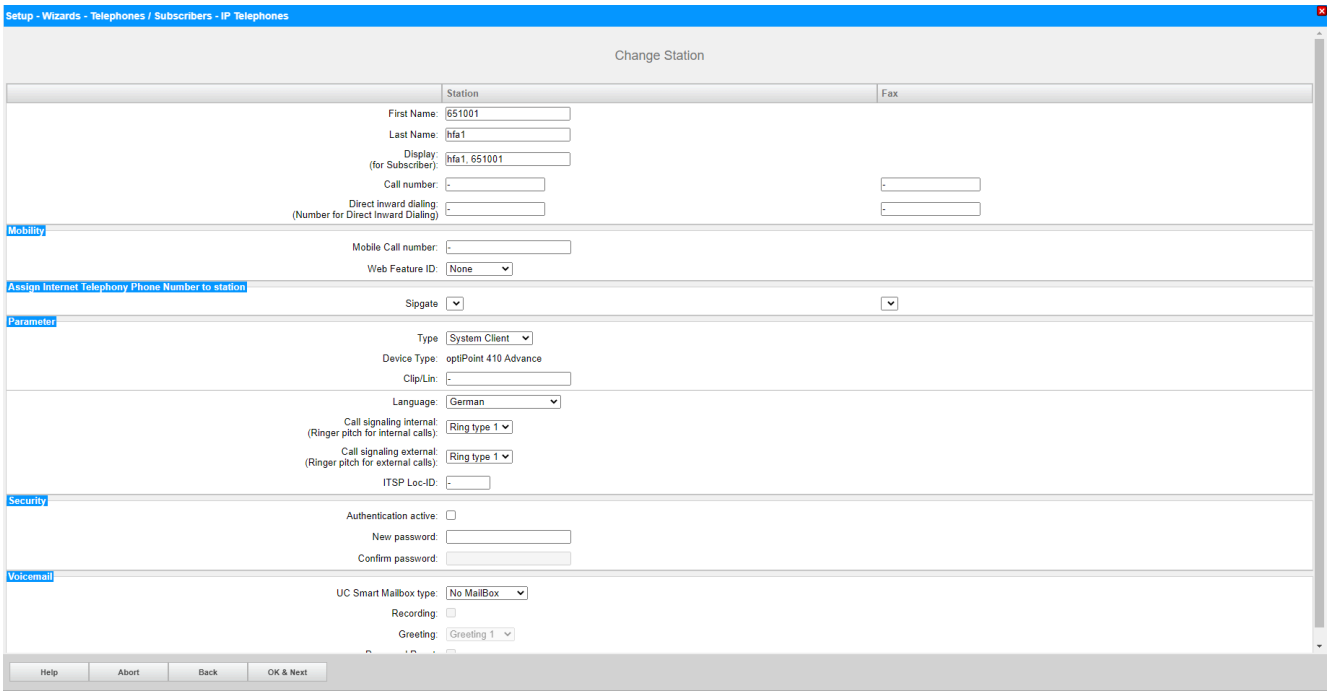
10) Choose the desired Class of Service group in the row of the desired subscriber from the **Class of Service** drop-down list.

11) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

12) If you want to change the DECT phone code (PIN), enter the new code in the row of the desired subscriber under **Mobile code**. The DECT subscribers must log on at the base station again with this code.

13) Make any further settings if required:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is

formatted and sent as the Calling Party Number for the external call.

d) Select the language for the menu controls on the phone from the **Language** drop-down list.
e) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).
f) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).
g) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
h) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
i) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.
j) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

k) Click on **OK & Next**.
l) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.
m) Click on **OK & Next**.

14) If you want to configure another station, repeat steps 5 through 13.
15) Click on **OK & Next**. A list of all configured DECT stations appears. If required, you can print the list of DECT stations with **Print**.
16) Click on **OK & Next** followed by **Finish**.

Related tasks

How to configure DECT Phones for the First Time on page 922

11.13.5 How to Configure Mitel SIP DECT Stations through Provisioning

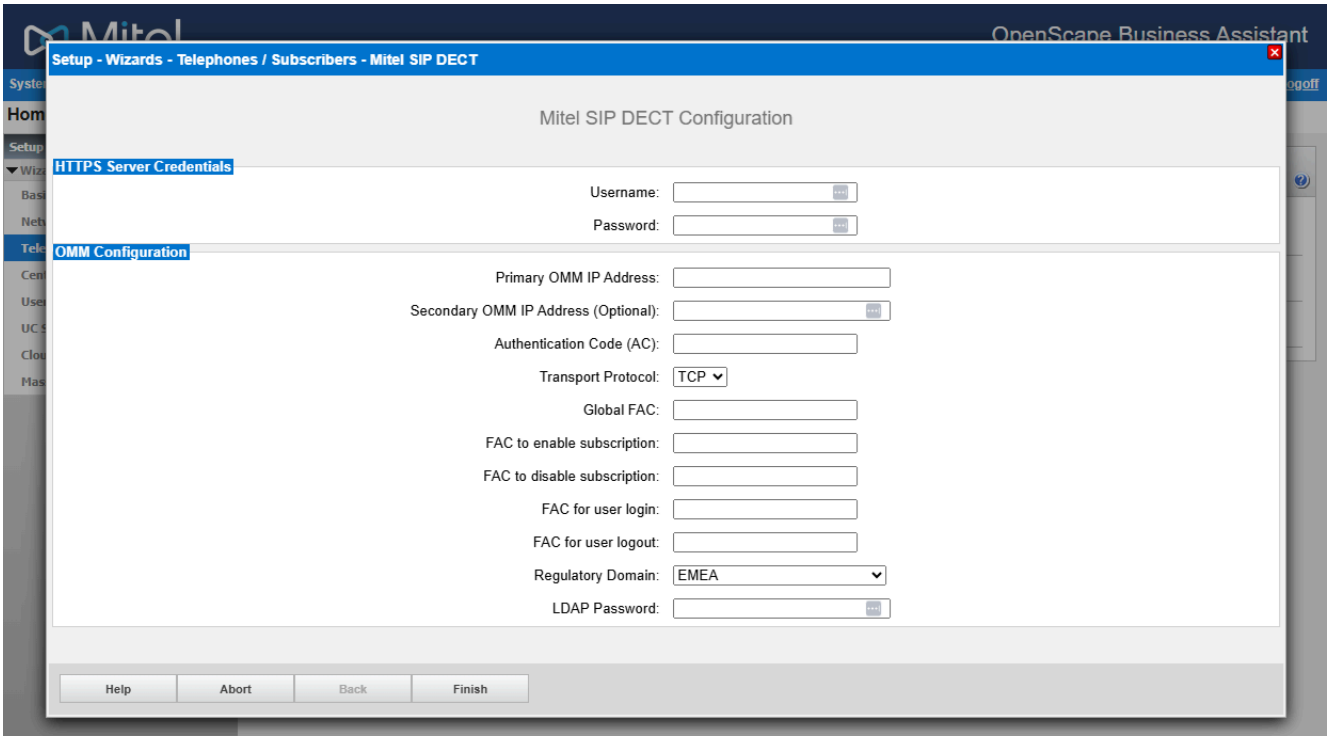
You can use the **Mitel SIP DECT** wizard to configure the Mitel SIP-DECT devices and connect to the Open Mobility Manager (OMM).

Prerequisites

The MAC address for the SIP DECT RFP device is known.

Step by Step

1) In the navigation bar, click on **Expert Mode > Network Interfaces > DHCP**.
2) Click to enable **DHCP Server**.
3) In the navigation bar, click **DHCP Server > Static IP Addresses**.
4) In the **Static IP Addresses** window, click on the **Add Static IP Address** tab.
5) Enter the required information as described in Network Interfaces > Mainboard> DHCP Mode > DHCP Server > Static IP Addresses.
6) Click **Apply**.
7) In the navigation bar, click **Setup**.
8) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
9) Click on **Edit** to start the **Mitel SIP DECT** wizard.



10) Under **HTTPS Server Credentials**, provide the credentials to access the server.
    a) Set the **Username** and **Password**.
11) Under **OMM Configuration**:
12) Provide the **Primary OMM IP Address** and **Secondary OMM IP Address (Optional)** IP address of the OMM.
13) Set the **Authentication Code (AC)**.
14) In **Transport Protocol**, choose one of the following values from the drop-down menu:
    - TCP
    - UDP
    - TLS

15) Set the various Feature Access Codes (FAC) under the following fields:
    a) **Global FAC**
    b) **FAC to enable subscription**
    c) **FAC for user login**
    d) **FAC for user logout**
16) In **Regulatory Domain**, choose one of the following values from the drop-down menu:
    - EMEA
    - US
    - Brazil
    - Taiwan
    - Radio 1910 - 1927 MHz 250 Mw
17) Provide the **LDAP password** to access the OpenScape Business internal user directory.
18) Click **Finish**.
    The configuration files needed from the OMM application are generated.
19) Configure a SIP station as described in How to Configure SIP Stations via Expert Mode.
20) Connect the Mitel SIP DECT RFP device to the network. Wait for a few moments for the device to receive an IP address from the DHCP server.
21) Connect to the OMM application and configure the base station, as described in the "*Mitel SIP DECT Phone Configuration Guide*".

11.13.5.1 How to Configure SIP Stations via Expert Mode

You can use **Expert Mode** to configure the SIP stations.

Prerequisites

You are logged on to the WBM with the **Expert** profile.

Step by Step

1) In the navigation tree, click **Expert Mode** > **Telephony Server** > **Station**.
2) In the new window, click to expand **Station** and then select **IP Client**. A list of all IP/SIP stations appears.
3) In the **Type** column, select **SIP Client**.
4) Click **Apply**.
5) Click the blue arrow, next to the IP station call number, under the **CallNo** column.
6) In the **Edit station parameters** window, select **Mitel SIP DECT Device** from the drop-down menu in **Device Provisioning**.
   The **Mitel SIP DECT Configuration** option appears.
7) Under **Mitel SIP DECT Configuration** option, set the following:
    a) Enter the device's **PIN**.
    b) In **Key Lock Enabled**, enable (Yes) or disable (No) the device key lock.
    c) In **Key Lock PIN** enter the PIN for the key lock.
    d) In **Key Lock Time** enter the time for the key lock PIN to take effect.
    e) In **Show Personal Directory** choose whether the personal directory is visible (Yes) or not (No).

8) Click **Apply**.
9) Navigate to the **Edit workpoint client data** tab.
10) Under **Parameters**, configure the values as described in Station Parameters.
11) Click **Apply**.

11.13.6 How to Configure ISDN Stations

The **ISDN Devices** wizard can be used to configure the ISDN stations (e.g., ISDN phone or ISDN fax).

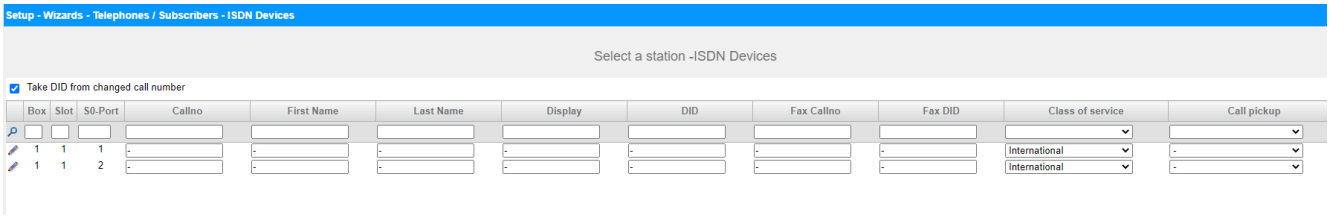
Prerequisites

At least one free S_0 interface is available. If one of the S_0 ports of a hardware platform is used, this must be set up as an internal S_0 port.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click on **Edit** to start the **ISDN Devices** wizard. A list of all ISDN stations appears.



4) If you want the direct inward dialing number of the station to be automatically adapted to its call number, activate the radio button **Take DID from changed call number**.
5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:
   - Only for a point-to-point connection:

     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.

6) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.

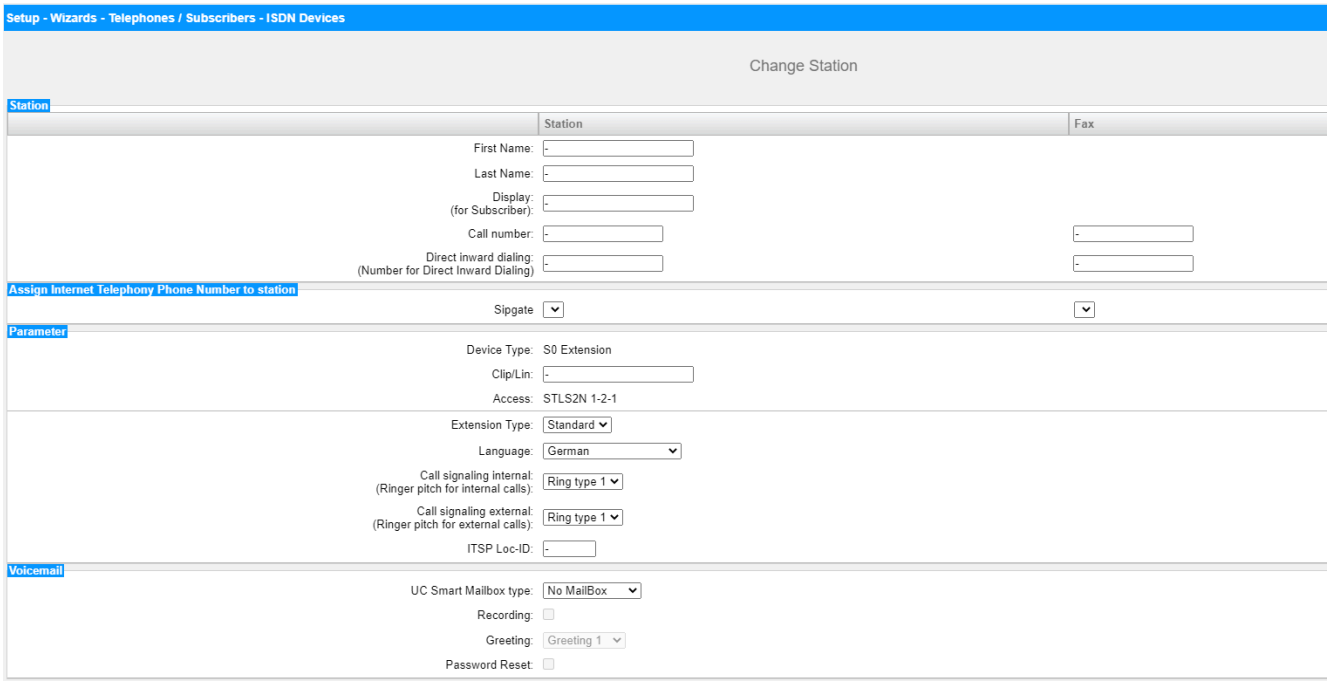
7) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.

8) Choose one of the Class of Service groups in the row of the desired subscriber from the **Class of Service** drop-down list:

9) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

10) Make any further settings if required:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is

formatted and sent as the Calling Party Number for the external call.

d) Select the type of ISDN terminal from the **Extension Type** drop-down list (`Standard` or `Fax`).
e) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for ISDN terminals.
f) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).
g) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).
h) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
i) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
j) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.
k) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

l) Click on **OK & Next**.
m) Change the station flags as needed. For a description of the station flags, see Station > Station > Station Parameters.
n) Click on **OK & Next**.

11) If you want to configure another station, repeat steps 5 through 10.
12) Click on **OK & Next**. A list of all configured ISDN stations appears. If required, you can print the list of ISDN stations with **Print**.
13) Click on **OK & Next** followed by **Finish**.

11.13.7 How to Configure Analog Stations

You can use the **Analog Devices** wizard to configure analog stations (e.g., analog phone or fax).

Prerequisites

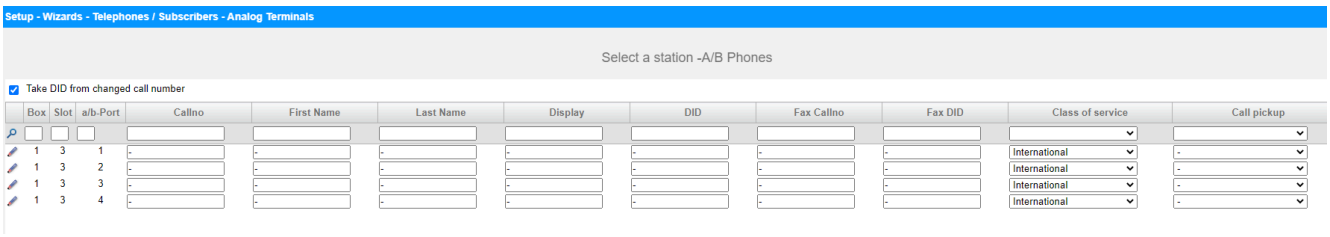
At least one free analog interface is available.

DTMF is enabled at the analog devices.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click on **Edit** to start the **Analog Terminals** wizard. A list of all analog stations appears.



4) If you want the direct inward dialing number of the station to be automatically adapted to its call number, activate the radio button **Take DID from changed call number**.
5) If you want a different direct inward dialing number for the station than the call number, enter a DID number for the station under **DID** in the row of the desired station:
   - Only for a point-to-point connection:

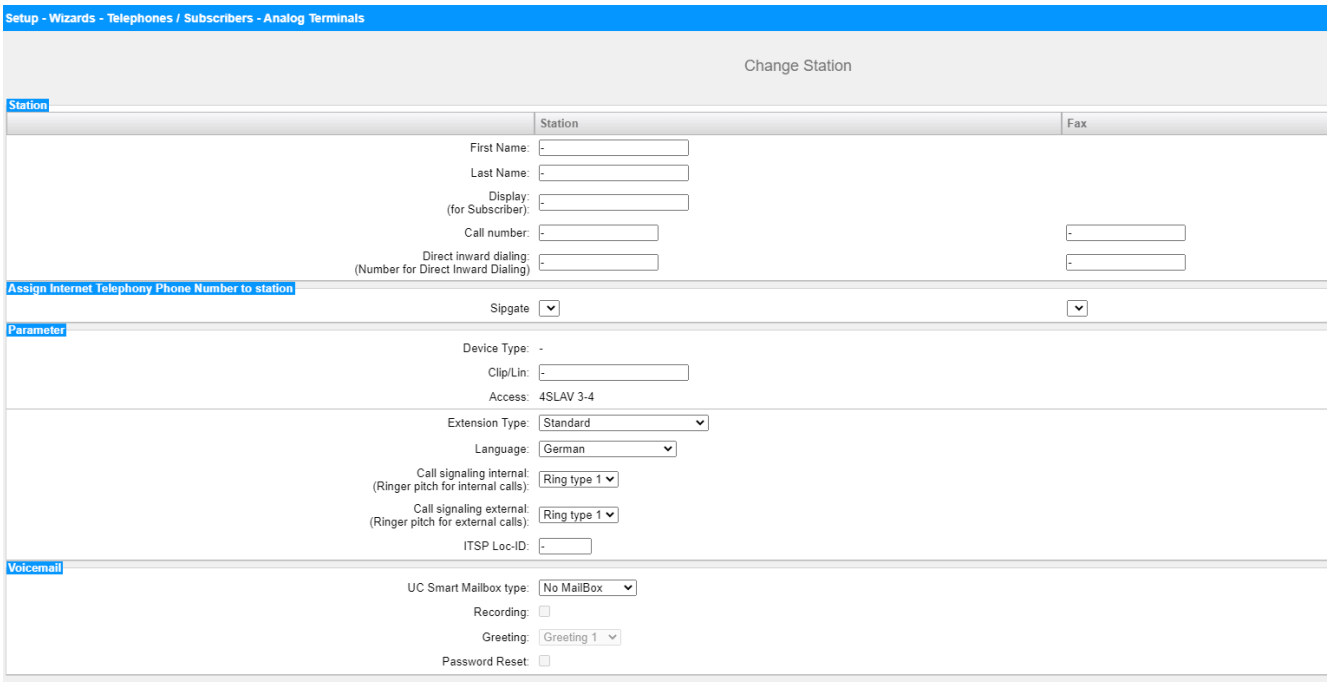
     Click in the desired field and type in the DID number using the keyboard. The DID number may also be identical to the internal station number.
   - Only for a point-to-multipoint connection:

     Select an MSN in the desired field via the drop-down list. The station can be internally reached via the internal station number 101, for example, and externally via the MSN 654321.
   - For point-to-point and point-to-multipoint connections:

     Select the entry **xxx - modifiable** (xxx is the internal station number) via the drop-down list in the desired field and type in the DID number using the keyboard or select an MSN from the drop-down list.
6) Enter the internal station number for the subscriber under **Call No** in the appropriate row of the desired subscriber. You can use the preset phone number or assign some other free number.
7) In the row of the desired station, under **Name**, enter a name in the format `Last Name, First Name` or `First Name Last Name`.
8) Choose one of the Class of Service groups in the row of the desired subscriber from the **Class of Service** drop-down list:
9) To add the subscriber to a call pickup group, select a call pickup group from the **Call pickup group** drop-down list in the row of the desired subscriber.

10) Make any further settings if required: - For an analog modem, the station type **Modem** must be selected here:

a) Click in the row of the desired station on the pencil icon **Edit**.



b) Select a DID number from the drop-down list in the **Direct inward dialing for Internet Telephony** area. A drop-down list is displayed for every active ITSP.

NOTICE: The **DID for Internet Telephony** field is not visible if Internet telephony is not configured or if no Internet Telephony Service Provider has been activated.

---

c) In the **Clip/Lin** field, enter a phone number (DID number or MSN) to be displayed at the called party's extension instead of the own phone number in the case of an external call.

NOTICE: This feature must be released by the network provider.

NOTICE: At least one DID number should be configured. If not, the system does not take into account caller's CLIP number and the internal call number is

formatted and sent as the Calling Party Number for the external call.

d) Select the analog terminal type (fax, for instance) in the **Extension Type** drop-down list.

If an analog modem is to be set up, the station type **Modem** must be selected here.

e) Do not change the default selection in the **Language** drop-down list. This setting has no relevance for analog terminals.

f) From the **Call signaling internal** drop-down list, select and assign one of a total of eight possible acoustic call signals for internal calls. The station then will then send the modified ringing tone to other internal stations, thus enabling its calls to be distinguished from other internal stations (default: Ring type 1).

g) From the **Call signaling external** drop-down list, select and assign one of a total of three possible acoustic call signals for external calls (default: Ring type 1).

h) Only with UC Smart: Select whether the subscriber is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.

i) Only with UC Smart and default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.

j) Only with UC Smart: Select a greeting from the **Greeting** drop-down list.

k) Only with UC Smart: If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

l) Click on **OK & Next**.

m) Change the station flags as needed. For a description of the station flags, see Station>Station>StationParameters .

n) Click on **OK & Next**.

11) If you want to configure another station, repeat steps 5 through 10.

12) Click on **OK & Next**. A list of all configured analog stations appears. If required, you can print the list of analog stations with **Print**.

13) Click on **OK & Next** followed by **Finish**.

11.13.8 How to Edit Station Names

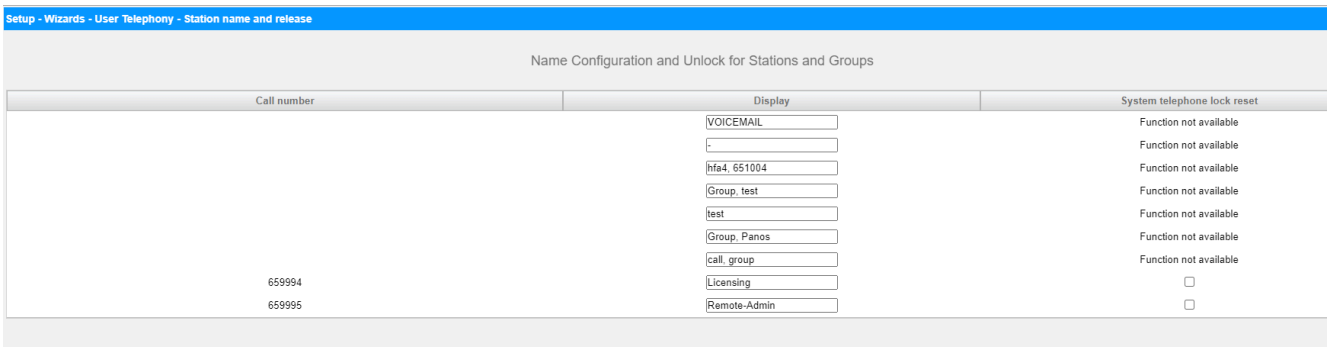
The **Station Name and Release** wizard can be used to edit the names of stations.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Name and Release** wizard.



4) Click in the **Display** column in the field of the desired subscriber and edit a subscriber name in the format `Last Name, First Name` or `First Name Last Name`.
5) If you want to edit the names of further stations, repeat step 4.
6) Click on **OK & Next**, followed by **Finish**.

11.14 Configuring Station Profiles

The values and properties of IP stations are stored in station profiles.

Using the **Profiles** wizard, an administrator with the **Advanced** profile can perform the following configuration tasks:

- Create a new profile
- Display profiles and their members
- Add members to a profile
- Delete members from a profile
- Export or import a single profile

In Expert mode, an administrator with the **Expert** profile can also perform the following configuration tasks:

- Change values and settings of a station profile
- Export or import all profiles

Station profiles that have already been created cannot be deleted, but can be overwritten.

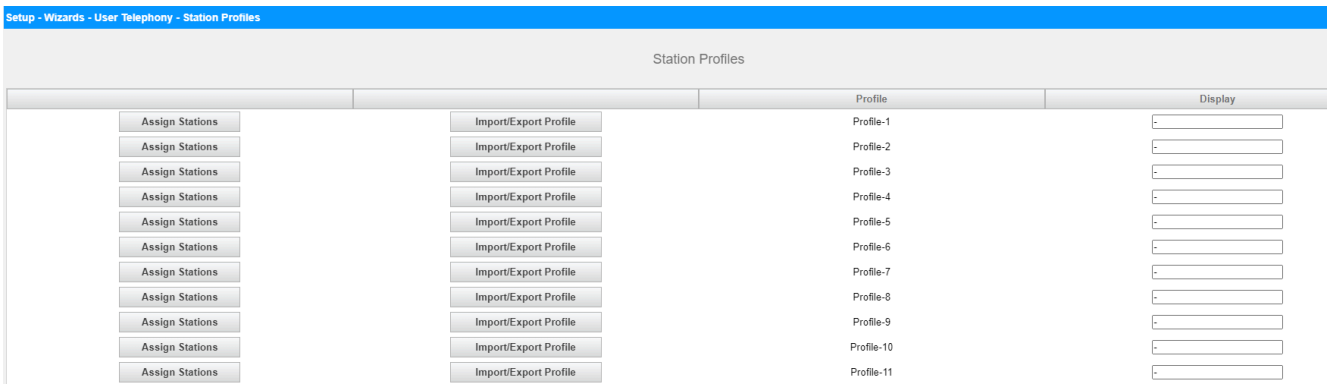
11.14.1 How to Create a New Station Profile

Prerequisites

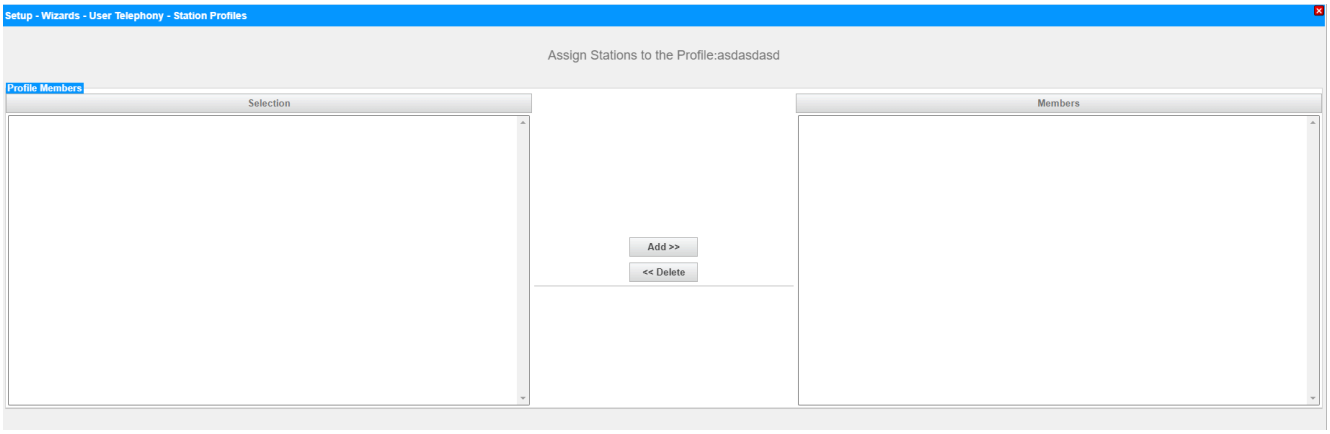
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Profiles** wizard. All existing station profiles are displayed.



4) In the row of the desired station profile, in the **Display** column, enter a name of your choice for the profile (max. 16 characters).
5) Click **Assign Stations** in the row of the desired station profile.



6) Select the desired members from the **Profile Members** table (multiple selections are allowed) and click on **Add**. These stations are now assigned to the station profile and cannot be assigned to any further station profile.
7) Click on **OK**.
8) Click on **OK & Next**. All existing station profiles and their members are displayed.
9) Click on **OK & Next** followed by **Finish**.

11.14.2 How to Display Station Profiles and their Members

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Profiles** wizard. All existing station profiles are displayed.
4) Click on **OK & Next**. All existing station profiles and their members are displayed.

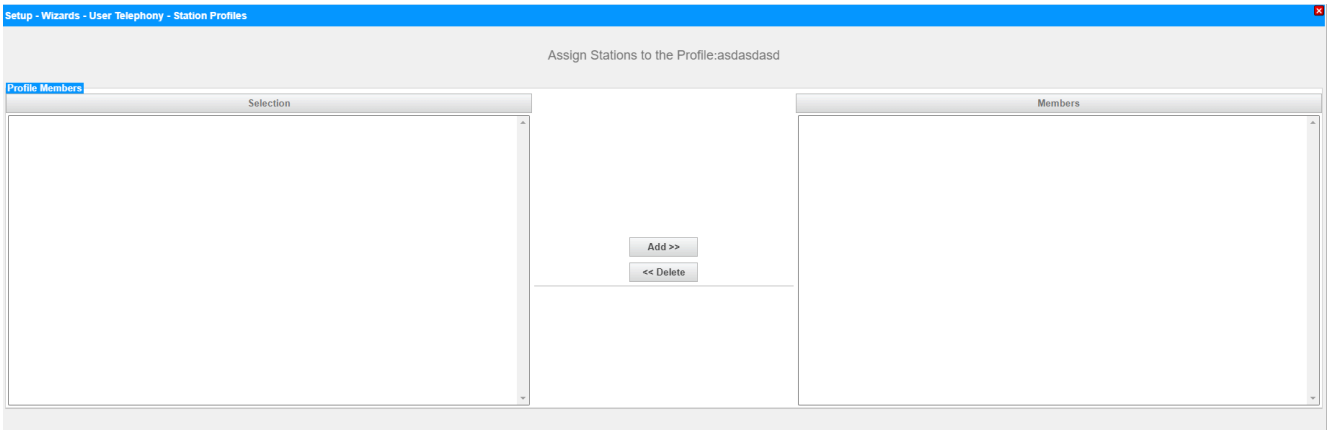
11.14.3 How to Add Members to a Station Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Profiles** wizard. All existing station profiles and their members are displayed.
4) Click **Assign Stations** in the row of the desired station profile.



5) Select the desired members from the **Profile Members** list (multiple selections are allowed) and click on **Add**. These stations are now assigned to the station profile and cannot be assigned to any further station profile.
6) Click on **OK**.
7) Click on **OK & Next**. All existing station profiles and their members are displayed.
8) Click on **OK & Next** followed by **Finish**.

11.14.4 How to Delete Members from a Station Profile

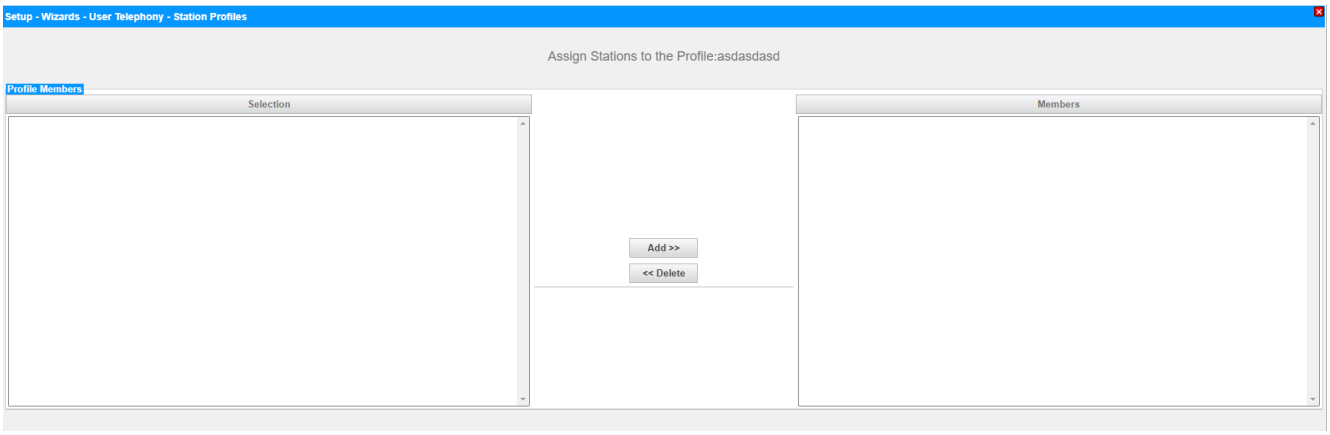
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Profiles** wizard. All existing station profiles and their members are displayed.
4) Click **Assign Stations** in the row of the desired station profile.



5) Select the desired members from the **Members** list (multiple selections are allowed) and click on **Delete**. These subscribers can now be reassigned to another station profile.
6) Click on **OK**.
7) Click on **OK & Next**. All existing station profiles and their members are displayed.
8) Click on **OK & Next** followed by **Finish**.

11.14.5 How to Export or Import a Single Station Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Station Profiles** wizard. All existing station profiles and their members are displayed.
4) Click **Import/Export Profile** in the row of the desired station profile.
5) If you want to export the station profile to a file, click on **Download** and save the file in a directory of your choice.
6) If you want to import a station profile from a file, click **Browse**, navigate to the storage location of the file and load the file into the communication system.
7) Click on **OK**.
8) Click on **OK & Next**. All existing station profiles and their members are displayed.
9) Click on **OK & Next** followed by **Finish**.

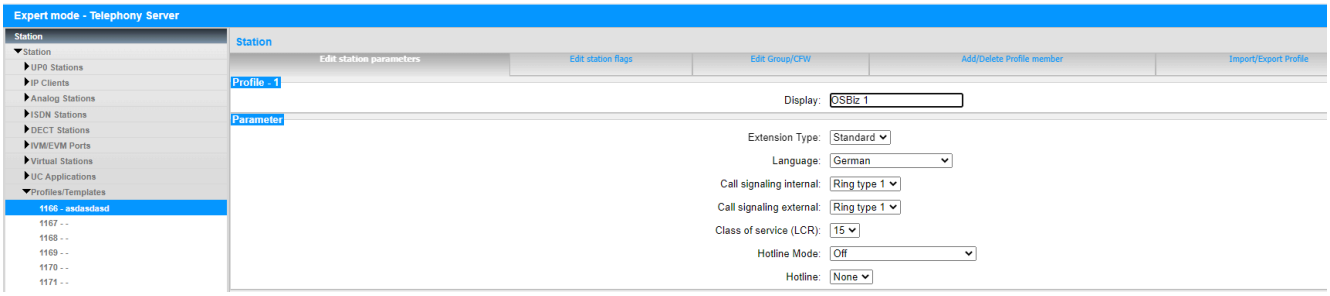
11.14.6 How to Change Values and Settings of a Station Profile

Prerequisites

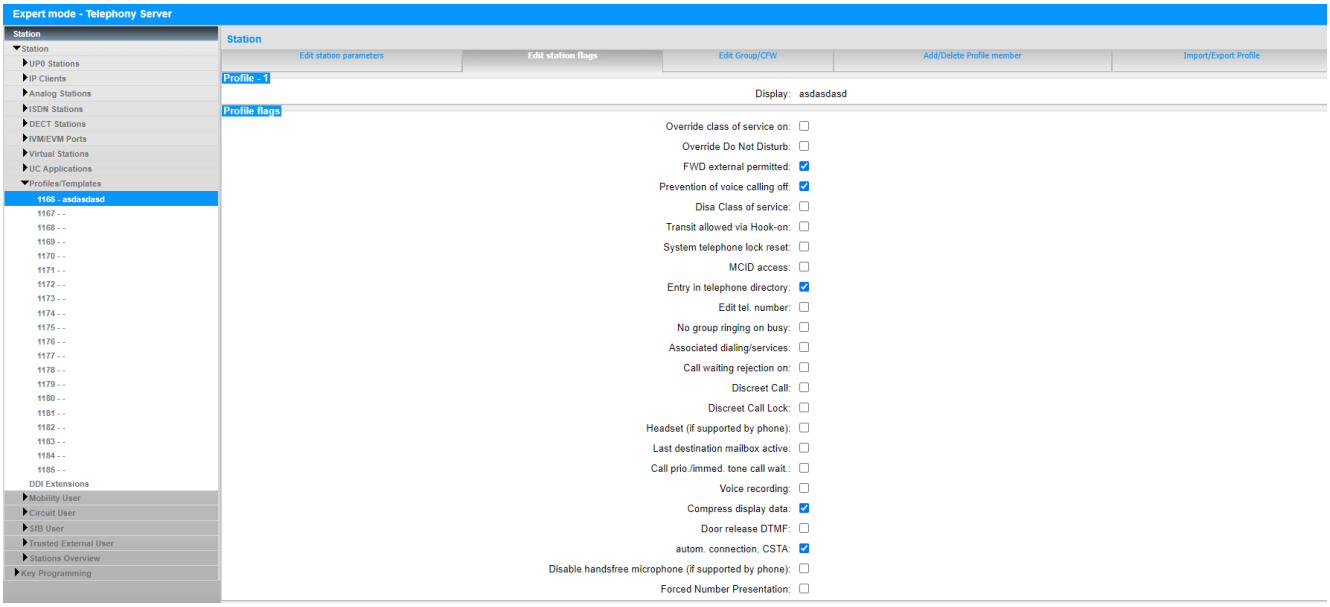
You are logged into the WBM with the **Expert** profile.

Step by Step

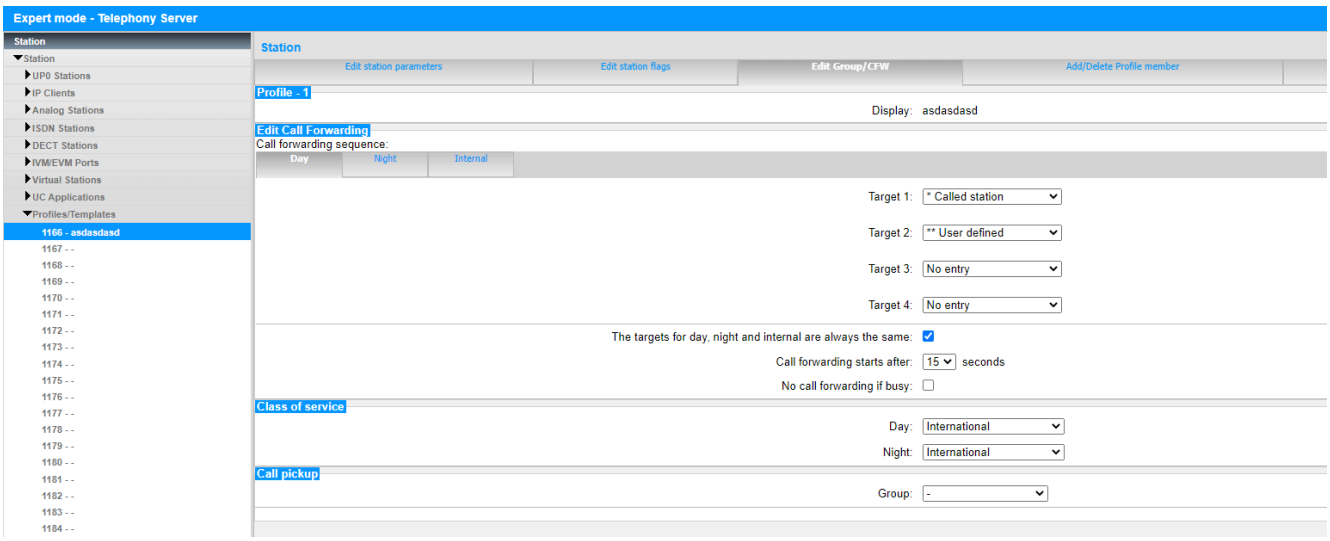
1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Stations**.
3) In the menu tree, click **Station** > **Profiles/Templates**.
4) In the menu tree, click on a station profile number.



5) If required, edit the name of the station profile (up to 16 characters are possible) on the **Station Parameters** tab in **Name** field and click **Apply**.
6) If required, edit the desired station parameters for the station profile on the **Station Parameters** tab and click **Apply**.



7) If required, edit the desired station flags for the station profile on the **Station Flags** tab and click **Apply**.



8) If required, edit the desired call forwardings for the station profile on the **Edit Group/CFW** tab and click **Apply**.
9) Click on **Apply**.

11.14.7 How to Export or Import all Station Profiles

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Stations**.
3) In the menu tree, click **Stations** > **Profiles/Templates**.
4) Click on the **Import/Export All Profiles** tab.
5) If you want to export all station profiles to a file, click on **Download** and save the file in a directory of your choice.
6) If you want to import all station profiles from a file, click **Browse**, navigate to the storage location of the file and load the file into the communication system.

11.15 Configuring the Authentication Data at the SIP Phone

The data used to authenticate a SIP subscriber at the communication system must also be entered directly at the SIP phone. The must be done by using the data that was entered in the WBM for each SIP subscriber.

The following data must be taken from the WBM and entered at the SIP phone (separately for each SIP phone):

- Password

  Password for authentication.
- SIP User ID / Username

  User name for authentication.
- Realm

  Zone or domain for authentication.

The configuration can be performed via the WBM of the SIP phone or directly on the display of the SIP phone.

11.15.1 How to Configure the Authentication Data via the WBM of the SIP Phone

Prerequisites

The SIP phone is integrated in the LAN.

The admin PC has access to the WBM of the SIP telephone.

You know the IP address of the SIP phone.

The configuration uses an OpenStage 60 SIP as an example.

Step by Step

1) Start the web browser on the admin PC and open the login page of the WBM of the SIP telephone at the following address:

`https://<IP address of the SIP telephone>`

NOTICE: If the WBM cannot be started, check the LAN connection and repeat the call. If it still cannot be started, check whether the IP address has been blocked by your firewall. More detailed information can be found in the documentation of your firewall

---

2) If the browser reports a problem with a security certificate, install the certificate (using the example of Internet Explorer V10).

a) Close the web browser.

b) Open the web browser with administrator rights by clicking the right mouse button on the web browser icon and selecting the menu item **Run as administrator** from the context menu.

c) Allow the User Account Control.

d) Open the login page of the WBM of the SIP telephone at the following address:

`https://<IP address of the SIP telephone>`

e) Click on **Continue to this website**.

f) Click on the message **Certificate Error** in the navigation bar of the web browser.

g) Click on **View Certificates**.

h) Click on **Install Certificate** (only visible with administrator rights).

i) Select the option **Local Computer** and confirm with **Next**.

j) Select the option **Place all certificates in the following store**, click **Browse** and specify **Trusted Root Certification Authorities**.

k) Confirm with **OK** and then with **Next** and **Finish**.

l) Confirm the certificate import with **OK** and close the certificate window **OK**.

m) Close the web browser.

n) Start the web browser again (without administrator rights) and open the login page of the WBM of the SIP telephone at the following address:

`https://<IP address of the SIP telephone>`

3) When you log in for the first time, you are prompted to enter a password.

a) Enter a new password in the **New Password** and **Confirm Password** fields to protect the system against misuse. Note case usage and the status of the **Num** key. The password is displayed as a string of asterisks (*).

NOTICE: The password must be at least 6 characters long and include a digit. Make sure that you remember your new password.

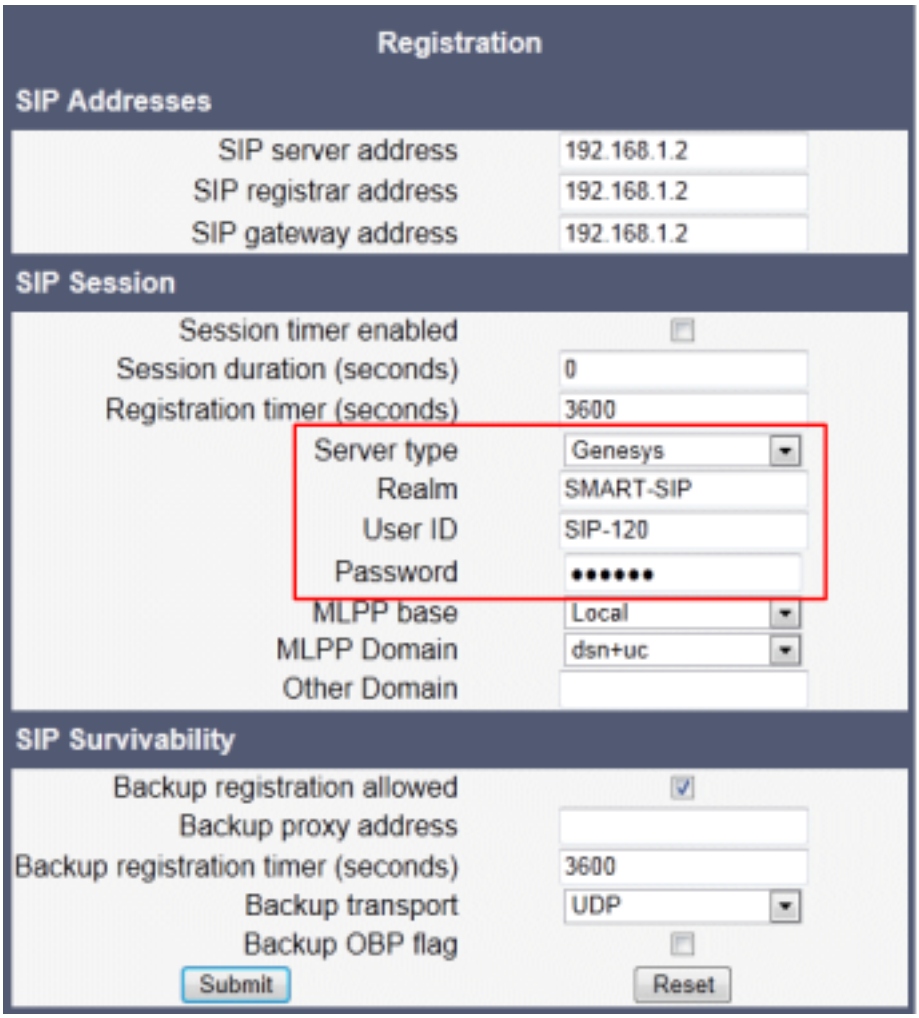
---

4) Click on **OK**.

5) Click on the **Administrator Pages (Admin)** tab.

6) Enter the administrator password (default password: 123456) and click **Login**.

7) Navigate to **System** > **Registration**.



8) Select the entry **Genesys** from the **Server type** drop-down list in the **SIP Session** area.

9) In the **Realm** field, enter the realm entry that you specified when configuring SIP stations in the WBM of the communication system (e.g., `SMART-SIP`).

10) In the **User ID** field, enter the user ID that you specified when configuring SIP stations in the WBM of the communication system (e.g., `SIP-120`).

11) In the **Password** field, enter the password that you specified when configuring SIP stations in the WBM of the communication system.

12) Click on **Submit**. The changes are saved.

13) Log out from the WBM with the **Logoff** button.

11.15.2 How to Configure the Authentication Data on the Display of the SIP Phone

Prerequisites

The required authentication data (user ID, password, and realm) is known to you.

The configuration uses an OpenStage 80 SIP as an example.

Step by Step

1) To reach the administration mode of the system telephone, press the appropriate key for the Settings/Applications menu on the phone.
2) Scroll through the `Settings` options until `Admin` and confirm this with the OK key.
3) Enter administrator password (`123456` by default) and confirm your selection with the OK key.
4) Scroll to `System` and confirm your selection with the OK key.
5) Scroll to `Registration` and confirm your selection with the OK key.
6) Scroll to `SIP Session` and confirm your selection with the OK key.
7) Scroll to `Server type` and confirm your selection with the OK key.
8) Scroll to the `Genesys` entry and confirm your selection with the OK key.
9) Scroll to `Realm` and confirm your selection with the OK key.
10) Enter the realm entry that you specified when configuring SIP stations in the WBM of the communication system (e.g., `SMART-SIP`). Click OK to confirm.
11) Scroll to `User ID` and confirm your selection with the OK key.
12) Enter the user ID that you specified when configuring SIP stations in the WBM of the communication system (e.g., `SIP-120`). Click OK to confirm.
13) Scroll to `Password` and confirm your selection with the OK key.
14) Enter the password that you specified when configuring SIP stations in the WBM of the communication system. Click OK to confirm.
15) After saving the changes, confirm the prompt by selecting `Save` select and confirming it with the OK button.
16) Use the Back key to go back to the `Admin` menu.
17) If the system telephone needs to be restarted due to the changes made, the menu item `Restart` will appear in the `Admin` menu. Confirm the `Restart` with the OK key and then also confirm `Yes` with the OK key. The system telephone performs a reboot and logs in to the communication system.

11.16 Exporting Subscriber Data

Important subscriber data can be exported to an XML file.

In addition to the user data, such as the names and phone numbers of the subscribers, e-mail addresses and phone types, for example, the XML file may also contain additional information such as group phone numbers and license assignments.

The XML file can be edited using a spreadsheet program such as Microsoft Office Excel, for example.

A template with sample data sets and a description thereof can be found in the file `csv-templates.zip` under **Service Center** > **Documents** > **CSV Templates**.

11.16.1 How to Export the Station Data

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Configuration** in the navigation tree.
3) Click on **Configuration** > **Port Configuration** in the menu tree.
4) Click on the **Export Configuration** tab.
5) Click on the **Download** button.
6) Confirm the prompt with **OK**.
7) Click on **Save** and select the storage location of the XML file.
8) Then click **Save**.

12 UC Smart

UC Smart is integrated in all OpenScape Business models (with and without the UC Booster) and offers unified communications features such as presence status and voice messages as well as conferencing, for example.

Clients for UC Smart

The UC Smart features can be used with the following clients:

- myPortal @work
- myPortal to go (as Mobile UC App or Web Edition)
- Application Launcher
- OpenScape Business Attendant / BLF
- 3rd Party WSI Clients

The capacity limits (for expansion) depend on the OpenScape Business model being used and any possibly installed OpenScape Business UC Booster variants.

Special Aspects of UC Smart with OpenScape Business S

Due to the system architecture, the following restrictions apply to OpenScape Business S:

- The number of voicemail messages is not shown on the phone's display (MWI).
- No fax, busy or idle detection is supported for the voicemail box (SmartVM). Incoming fax calls cannot be switched to a default fax device after being answered by the SmartVM. The SmartVM records for 2 minutes.
- When connections are switched by the Company AutoAttendant to busy subscribers, the caller receives a busy signal. There is no way to leave a voice message.
- If, when checking a voice message, you want to be redirected to the phone number stored in the SmartVM (calling party number), this number must be identical to the phone number of the user that was configured for the SmartVM.
- For connections to the voicemail box (SmartVM), SIPQ trunks are occupied at the UC Booster Server and OpenScape Business S. No trunk licenses are required for this.
- MEB channels are occupied for simultaneous announcements.
- Sixty MEB channels are available for voice connections to the voicemail box (SmartVM) or AutoAttendant.

NOTICE: After changes in configuration of Stations, Groups, Mobility or other system parameters like trunk access codes, the UC Data for either UC Smart or UC Suite need to be synchronized. Synchronization occurs five minutes after the last configuration change. If a later configuration change occurs before the 5 minutes timer, the timer is restarted. UC Data may outdated until synchronization starts.

Related concepts

UC Features (Overview) on page 87

12.1 Basic Settings for UC Smart

The basic settings for UC Smart can be customized.

UC Smart can be enabled or disabled. If UC Smart is used, UC Suite must be disabled.

Password Settings

The administrator must assign an initial password for all users of UC Smart and communicate this password to the users. The initial password may be the same for all users or different for each user. The initial password must be changed by the user when logging in at a UC Smart client for the first time. Without the assignment of an initial password, the user cannot log into to a UC Smart client.

The new password assigned by the user should meet stringent password policies.

Advanced Settings for Application-controlled Conferences (Optional)

During the basic installation, the administrator must set up the **Functional number for MeetMe Conferencing** (MeetMe dial-in number) and at least one **Functional number for Conferencing** (conference room) in the WBM.

For OpenScape Business X systems, the MeetMe dial-in number must be assigned a call destination list in which the first entry is empty and the second entry matches the call number of the voicemail box (SmartVM).

For OpenScape Business S systems, the MeetMe dial-in number must be assigned a call destination list in which the first entry matches the call number of the voicemail box (Route: Application Suite).

Finally, the MeetMe dial-in number must also be assigned a standard voicemail box.

The description of the configuration can be found here: How to Configure Application-controlled Conferences ,

License Assignments

The administrator must assign a UC User license to each UC Smart user.

Additional licenses can be optionally assigned for:

- Voicemail (also usable without UC Smart)
- Conference
- Application Launcher

12.1.1 How to Activate UC Smart

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click in the navigation tree on **Applications** > **Application Selection**.
3) If you want to use UC Smart without the UC Booster Server, click on **Package with UC Smart**,

4) If want to use UC Smart with the UC Booster Server, click on **Package with UC Smart on OSBiz UC Booster Server** and, in addition, enter the IP address of the external Linux server in the **IP address of the OSBiz UC Booster Server** field.
5) Click on **Apply**.

Next steps

How to Configure UC Smart

12.1.2 How to Configure UC Smart

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **UC Smart**.
3) Click on **Edit** to start the **UC Smart** wizard.
4) Click on **Administration** > **Basic Settings** in the menu tree.
5) Under **Enable / Disable UC Smart**, select the check box **Active**.
6) Assign initial password under **Password Policy**:
   a) Go to **System-wide initial UC Smart Password**, and click **Configure**.
   b) Enter the initial password for all UC Smart users in the **System-wide initial UC Smart password** field..
   c) Click on **Apply**.
7) Specify password policies under **Password Policy**:

   NOTICE: For detailed information on the password policies, click on the icon **i**.

   - If you want to enforce a strict password policy for user passwords (recommended), select the check box **Force user to choose secure password**.
   - If you do not want to enforce a strict password policy for user passwords (not recommended), clear the check box **Force user to choose secure password**.
8) Specify access to the system under **Access Rules**:
   - If you want to enable encrypted access from UC Smart clients to the system (recommended when using myPortal to go via the Internet), select the **HTTPS** check box.
   - If you want to enable unencrypted access from UC Smart clients to the system (not recommended when using myPortal to go via the Internet), select the **HTTP** check box.
9) Select the check box **Save login data for devices** if the login credentials are to be additionally stored in the phone.
10) Click on **Apply**.

12.1.3 How to Configure Application-controlled Conferences

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click on **Edit** to start the **Basic Installation** wizard.
3) Skip the **Overview** window with **OK & Next**. The **Central Functions for Stations** window appears.
4) Enable the radio button **Change pre-configured call and functional numbers**.
5) Click **Execute function**. The **Change preconfigured call and functional numbers** window appears.
6) If necessary, change the **Functional number for MeetMe Conferencing** to suit your requirements.
7) Assign at least one **Functional number for Conferencing** for the conference room.
8) Click **OK** when finished. You are taken back to the **Central Functions for Stations** window.
9) Click **OK & Next**.
10) Exit the wizard by skipping all other windows with **OK & Next**.
11) In the navigation bar, click on **Expert Mode**.
12) In the navigation tree, click **Telephony Server** > **Incoming Calls**.
13) Click **Incoming Calls** > **Call Forwarding** in the menu tree.
14) Click on the **Call dest. list - Definition** tab.
15) For OpenScape Business X, you define the call destination list for the MeetMe dial-in number as follows:
    a) Under **Call dest. list**, select a free call destination list, e.g., `500`.
    b) Select **No entry** as the first destination and select the call number of the voicemail box (e.g., `351 VOICEMAIL Group`) as the second destination.
16) For OpenScape Business S., you define the call destination list for the MeetMe dial-in number as follows:
    a) Under **Call dest. list**, select a free call destination list, e.g., `500`.
    b) Select External Destination as First Destination (Route: Application Suite) and enter the call number of the voicemail box in "External Destination" field.
17) Click on **Apply** followed by **OK**.
18) Close the window.
19) In the navigation bar, click on **Expert Mode**.
20) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
21) Click on **Auxiliary Equipment** > **SmartVM** in the menu tree.
22) Click on the **Edit SmartVM Mailboxes** tab.
23) In the **Mailbox call no.** column, enter the MeetMe dial-in number for which the mailbox is to be added in any free field.

24) Click on **Apply** followed by **OK**.

12.1.4 How to Determine the IP Addresses of the System Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click in the navigation tree on **Applications** > **Application Selection**.

Under **Application Selection**, the IP addresses of various components are shown, including, for example, **UC Smart**, **Application Launcher**, **CSTA Connector**, **Open Directory Service**, **UC Suite** and **Web Collaboration**.

Related concepts

Basic Settings for UC Suite on page 512

12.1.5 How to Determine the Status of C Smart

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click on **Wizards** > **UC Smart**.

3) Click on **Edit** to start the **UC Smart** wizard.

4) Click on **Administration** > **Status** in the menu tree.

Status information on UC Smart is displayed under **Application Server**, including, for example: **Status**, **Version**, **Telephone System**, **Database**, **EVM**, **Pending Monitors**, **Active Users**, **Active Connections**, **Active HTTPS Connections**, **Mobility Entry Users**, **Users Without Device** and **Blocked Users**.

12.2 UC Smart Clients

UC Smart clients provide subscribers with convenient user interfaces for unified communications.

The system offers the following UC Smart clients for the following devices:

Client type	Client	Device
Communications Client	myPortal @work	PC

Client type	Client	Device
Mobile Client	myPortal to go (UC Smart) (see Mobility on page 898)	Smartphone, Tablet PC
Communications Client	OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA(integrated Client to phone software)	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA

12.2.1 myPortal @work

myPortal @work is a Unified Communication Application (Microsoft Windows and Mac OS X), which combines all needed features and services, like convenient dialing via phone directories, favorites, conversations and information on the presence status of colleagues, into a single solution designed to accelerate daily communication, improve teamwork and to get in quick contact with colleagues, customers and Partners.

myPortal @work can be used either in UC Smart or in UC Suite mode. Depending on the mode, the offered features in the user interface vary. You cannot change the operation mode, as this is set by the system administrator. In case of any doubt about the current operation mode of your myPortal @work client, ask your system administrator for details.

myPortal @work offers an embedded Voice over IP (VoIP) telephony client. If the VoIP option is activated, the voice call related features of the myPortal @work client use the VoIP functionality.

NOTICE: To use Voice over IP (VoIP) functionality, the user must be configured as system client.

For remote Voice over IP (VoIP) usage with Device@Home, please see 1 Configuration for System Device@Home

---

VoIP functionality supports a set of features on top of UC features:

- Make a call
- Answer a call
- Terminate a call
- Consultation
- Transfer after answer
- Blind transfer
- Deflect
- Deflect to voicemail
- Automatic Recall (display notification for a recall is not yet supported)
- Toggle/Connect
- Mute/Unmute (only for VoIP functionality)
- System Conference
- Call waiting rejection
- Camp-on
- Do not disturb (DND)
- DTMF

- Call pick up

> **NOTICE:** Since myPortal@Work client is not supporting the capability to send DTMF tones to another station, sending a DTMF tone via CSTA's command 'generateDigits' is respectively also not supported and such a request will be denied and rejected by the system.

Working in a team:

myPortal @work VoIP client can be also used in:

- Group (e.g. Linear, Call waiting)
- MULAP as a MULAP member

Signaling and Payload Encryption (SPE) is also supported for the communication system. VoIP client uses modern WebRTC security stack so it has also secure data transfer using DTLS.

> **NOTICE:** ITSP SDES configuration is also supported.

Service codes can be initiated from the search bar but they are not supported in case of problems. Feedback regarding successful or unsuccessful execution of service codes is not provided and thus, it is strongly advised to utilize the input options provided by the myPortal @work user interface in order to control the respective features.

myPortal @work in UC Suite Mode can be used not only as stand-alone but also in combination with existing myPortal for Desktop/Outlook, myAgent, myAttendant Client (CTI, Favorites and Conversations). The existing UC user licenses can also be used with myPortal @work.

The following description refers mainly to my Portal @work in UC Smart mode. Deviations for the UC Suite mode are pointed out in myPortal @work User Guide.

myPortal @work supports generally the following features:

- Presence status
- Status-based call forwarding
- Directories including search by name
- Favorites
- Conversations: up to 25 conversations are displayed in the client and each conversation has up to 50 entries
- Conferencing
- Hotkey Dialing / Hotkey Search / Telephony hyperlinks
- Call Functions either via:
  1) Associated telephone device
  2) Integrated Voice over IP telephony client
- Voicemail control
- Zoom In / Zoom Out
- Screen share via OpenScape Web Collaboration (optional)

Use of myPortal @work in Microsoft Terminal Server environment

myPortal @work is released for UC and CTI functionality in Microsoft Terminal Server environments with the following limitations:

- Telephony Hyperlinks and Click to Dial are not supported
- Start application on launch is not supported
- Upload of user image is not supported
- Functionality of dock/undock, pin/unpin and minimize to tray bar is limited
- VoIP functionality is not supported

12.2.1.1 Prerequisites for myPortal @work

In order to use the UC client, the client PC must be equipped with the appropriate hardware and software configurations. Depending on the configuration, administration rights are required for the installation and automatic updates. The available functionality depends on the licenses being used.

The following prerequisites are required for the installation of myPortal @work:

- Administrator rights
- myPortal @work software setup program
- IP addresses and ports of the communication system
- FQDN or IP address, port for WAN connectivity (device@home)
- Login Data (User and Password) for your UC user account in the communication system
- Voice-Mail account information (optional)
- MULAP call number in case of multiple number assignment (optional)
- Windows OS and Apple Mac OS X

NOTICE: Make sure that TLS 1.2 must be activated in Internet Options (in control panel) and the latest patches from Microsoft must be installed or activated manually.

If above actions are not performed then HTTPS access will be rejected.

Telephones

myPortal @work can be used in combination with the following telephones:

NOTICE: myPortal @work can also be used as stand-alone, using VoIP functionality, without the need of a physical device.

- 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
- Analog telephones
- ISDN Phones
- OpenScape Personal Edition HFA

- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Older devices (such as optiPoint 410/420/500 and Gigaset M2/SL3/S4/SL4/S5) are supported. Optiset E devices cannot be operated. For details on the tested and released devices, please refer to the Release Notice.

NOTICE: OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrated Client does not have any special prerequisites, apart from the standard client configuration and license.

"Favorites" in phone menu contains Free Programmable Keys and does not relate to UC Favorites. Details for those keys and how to, are available within the device documentation.

NOTICE: For analog and DECT telephones, the Message Waiting Indication (MWI) is not supported, and only limited support is available for displaying information on the phone.

Web Browsers

The following web browsers have been released for programming telephone keys via the UC client:

- Microsoft Internet Explorer Version 10 (or later)
- Mozilla Firefox Version 19 (or later)
- Google Chrome

Installation Files

The administrator can download the installation files from the **Service Center** > **Software** and make them available to users via a network drive, for example.

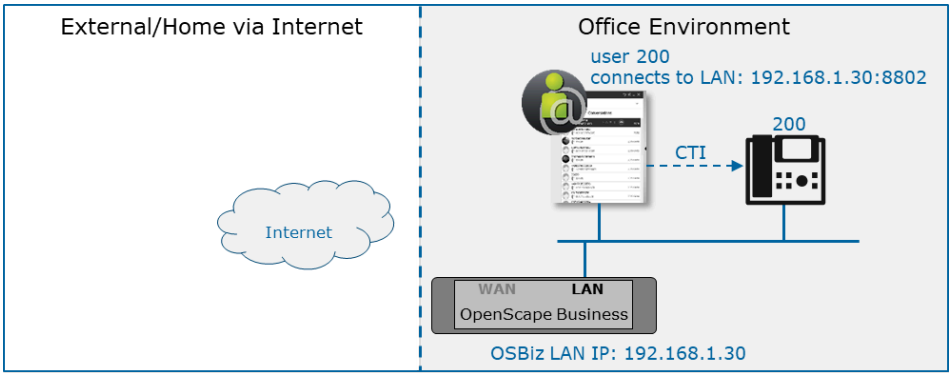
12.2.1.2 myPortal @work user configuration

myPortal @work is a combination of a UC client and a VoIP client and those two functionalities require the following configurations/licenses based on different UC modes (Smart/UC Suite) and use cases.

NOTICE: When a myPortal @work user account is locked after several incorrect log in attempts, in UC Suite mode, it is not visible in the UC Suite User Directory. You can view the locked myPortal @work users under **Expert Mode > Web Services > Web Services Assistant > User Management** but you can unlock these accounts under **Expert Mode > OpenScape Business UC Suite > User Directory**.

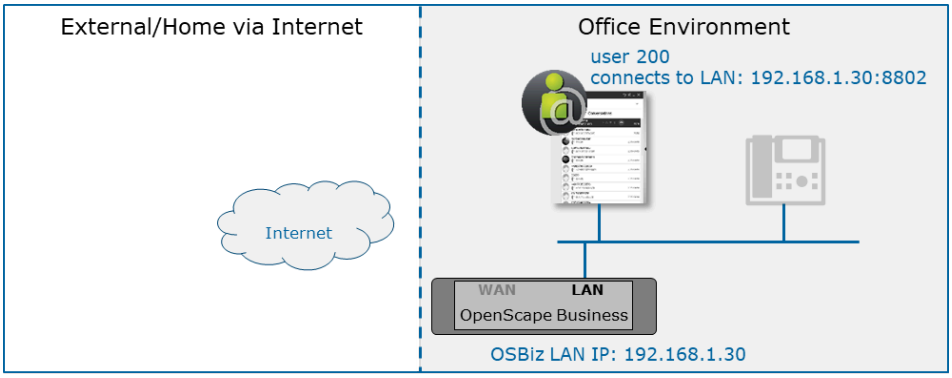
Local LAN configuration - UC and CTI client only

myPortal @work is used as UC and CTI client for an associated desk phone without VoIP.



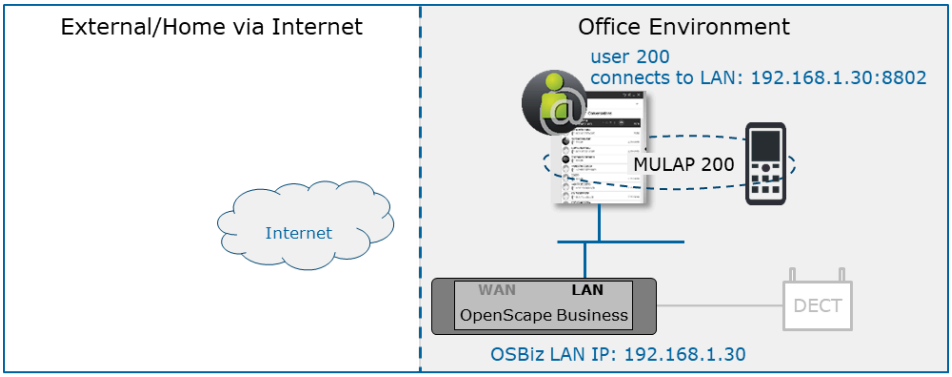
- Licenses: UC user or Groupware User
- myPortal @work login: in the login screen set your login username/ password / LAN IP address:8802

Local LAN configuration - UC and VoIP client



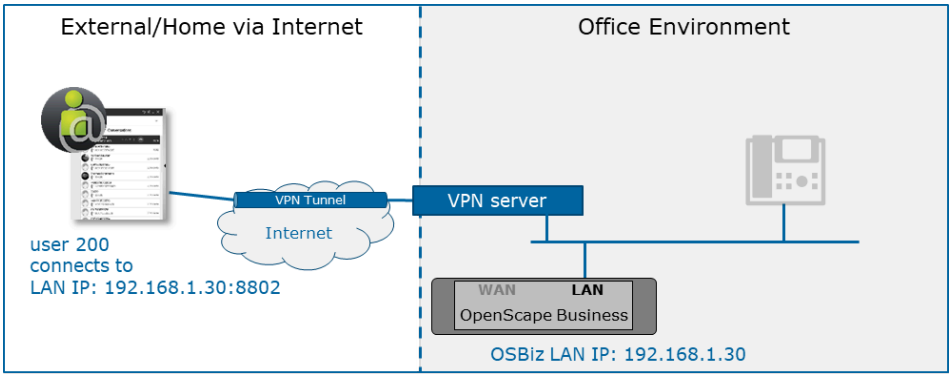
- Licenses: IP User and UC User or Groupware license
- myPortal @work login: in the login screen set your login username/ password / LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity in the client is not needed for pure inhouse connections. Nevertheless, this is required in some hybrid scenarios with other users using myPortal @work VoIP via pubic internet. In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

MULAP user configuration (Local LAN)



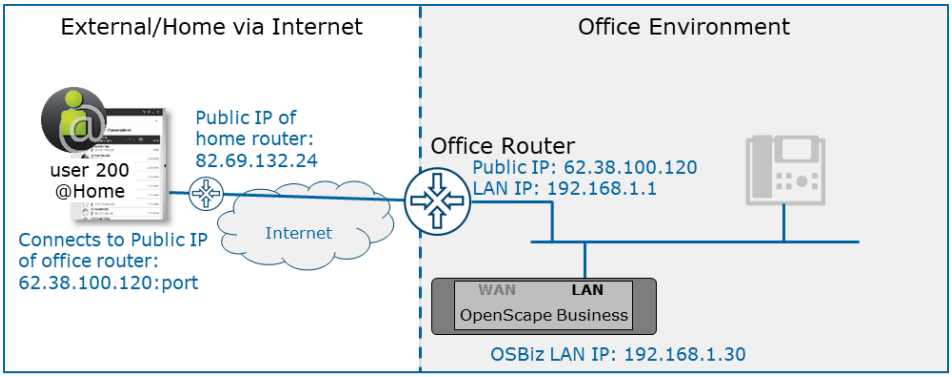
- Licenses:
  - myPortal @work: IP User and UC User or Groupware license
  - other Mulap device - in this example DECT: TDM User license or IP User (Mulap configuration is recommended for combination with TDM or DECT devices, but could also be used with an IP device. In case of an IP device see also section Deskshare user via local LAN on page 477 and Remote Deskshare user via VPN on page 477).
- myPortal @work login: in the login screen set your login username/password of the MULAP number / LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> choose the controlled device and then enable VoIP
- STUN connectivity in the client is not needed for pure inhouse connections. Nevertheless this is required in some hybrid scenarios with other users using myPortal @work VoIP via public internet. In order to check STUN connectivity, go to **Settings > VoIP > Advanced ICE settings > Check ICE status**.

Home user with VPN connection configuration



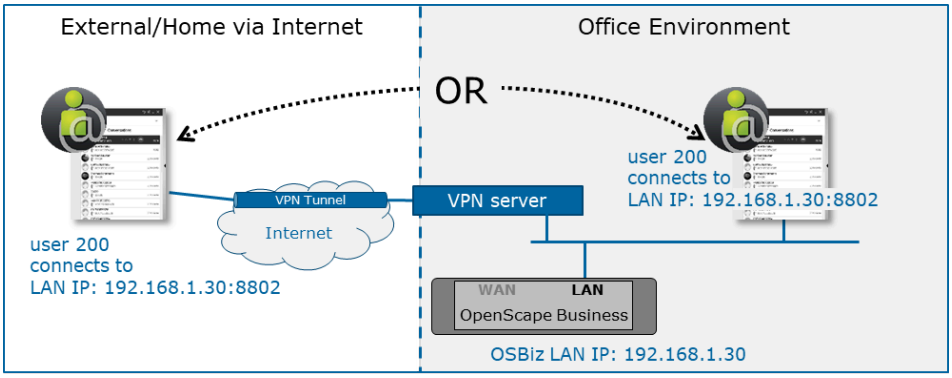
- Licenses: IP User and UC User or Groupware license
- myPortal @work login: in the login screen set your login username/ password / LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- STUN connectivity is mandatory. In order to check STUN connectivity go to Settings > VoIP > Advanced ICE settings > Check ICE status.

myPortal @work via public Internet



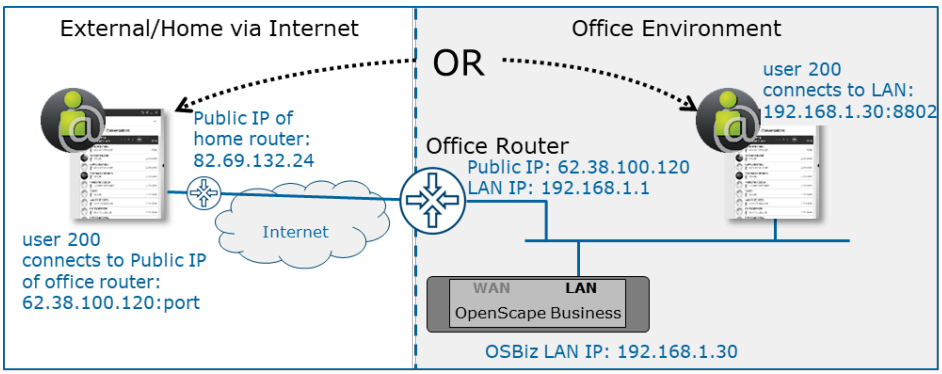
- Licenses: IP User and UC User or Groupware license
- myPortal @work login: in the login screen set your login username/ password / Public IP address:port configured from the administrator.
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- Prepare the network environment as described in chapter Configuration steps to use myPortal @work via the internet on page 479
- SBC flag is not required for myPortal @work. It is only needed if you use a Hardware device.
- Please do not use the OSBiz WAN interface for connecting to the internet when using myPortal @work via Public IP. If this is done internal SBC will detect the Public IP address of the WAN interface and will use this in the communication between the client and the OSBiz which will lead to payload issues. Proposed configuration: Connect the ITSP via the LAN interface. This can be done via the normal ISP router or via a second router and static routes.
- STUN connectivity is needed. In order to check STUN connectivity go to Settings > VoIP > Advanced ICE settings > Check ICE status.

Home user with VPN and local LAN configuration (e.g. Moving from office to home and back)



- Licenses: IP User and UC User or Groupware license
- myPortal @work login: in the login screen set your login username/ password/ LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- myPortal @work can be used in both environments without changing the settings.
- STUN connectivity is mandatorily needed. In order to check STUN connectivity, go to Settings > VoIP > Advanced ICE settings > Check ICE status.

myPortal @work via public Internet and local LAN configuration (e.g. moving from office to home and back)



- Licenses: IP User and UC User or Groupware license
- myPortal @work login: in the login screen set your login username/ password/ LAN IP address:8802 and Public IP address:port configured from the administrator. By configuring both addresses there is no need to use a second profile when moving from office to home and back.
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP
- Prepare the network environment as described in chapter Configuration steps to use myPortal @work via the internet on page 479
- SBC flag is not required for myPortal@work. It is only needed if you use a Hardware device.

For VoIP registration

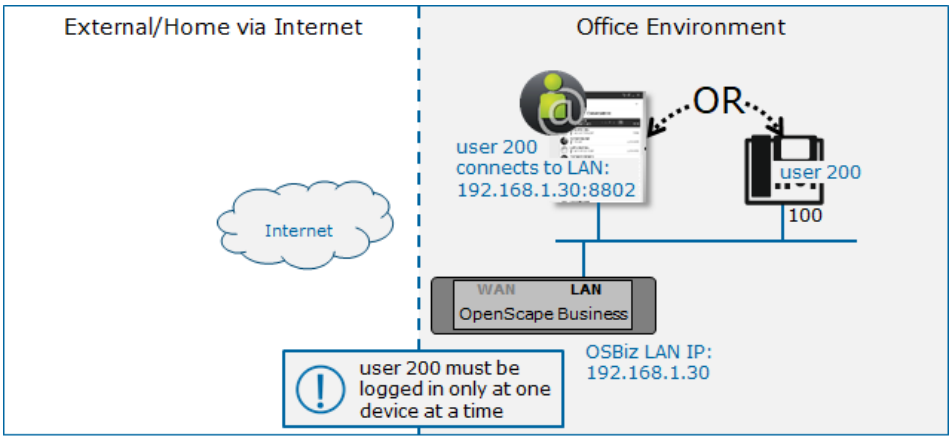
In case both local and home user are used, the user should have only one VoIP connection either in home or in office.

For UC

When the user wants to be connected in UC at the same time in more than one place:

- UC Smart mode: UC client can be connected at the same time from home and from office, but only one VoIP client is supported in this scenario and the VoIP functionality from the other client should be unregistered.
- UC Suite mode: Please check paragraph “Combination of myPortal @work with other UC Suite clients and license configuration” Only one myPortal @work client is allowed.

Deskshare user via local LAN



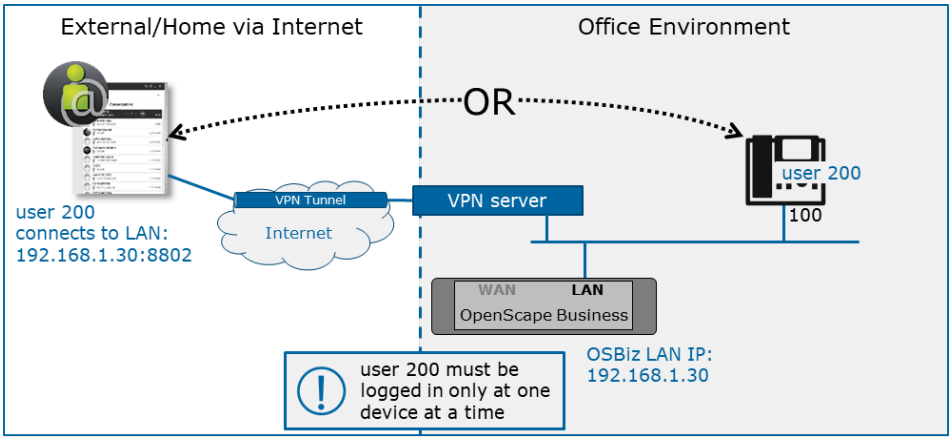
- Licenses: Deskshare license and UC User or Groupware license
- myPortal @work login: in the login screen set the login of the deskshare extension username/password/ LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP

Example: Device uses dummy number = “100” Connect to “100” with your DeskPhone as deskshare e.g. 200 using service code *9419.

In order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number “100”. When switching back to deskphone again please ensure that myPortal @work is unregistered (# user must exit the application or log out).

Remote Deskshare user via VPN

The same configuration as described in chapter Deskshare user via local LAN on page 477 is also supported for home user via VPN.



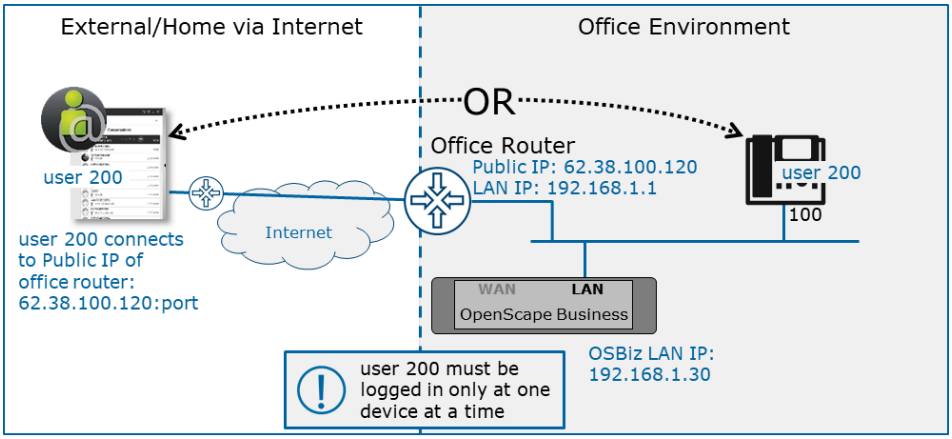
- Licenses: Deskshare license and UC User or Groupware license
- myPortal @work login: in the login screen set the login of the deskshare extension username/password/ LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP

Example: Device uses dummy number = “100” Connect to “100” with your DeskPhone as deskshare e.g. 200 using service code *9419.

In order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number “100”. When switching back to deskphone again please ensure that myPortal @work is unregistered (# user must exit the application or log out).

Remote Deskshare user via public Internet

The same configuration as described in chapter Deskshare user via local LAN on page 477 is technically also possible with home users via public Internet. Nevertheless, this is not yet completely tested and therefore described preliminary in this document version.



- Licenses: Deskshare license and UC User or Groupware license
- myPortal @work login: in the login screen set the login of the deskshare extension username/password/ LAN IP address:8802
- myPortal @work VoIP registration: After you have successfully logged in, you need to go to settings> VoIP> Enable VoIP

Example: Device uses dummy number = “100” Connect to “100” with your DeskPhone as deskshare e.g. 200 using service code *9419.

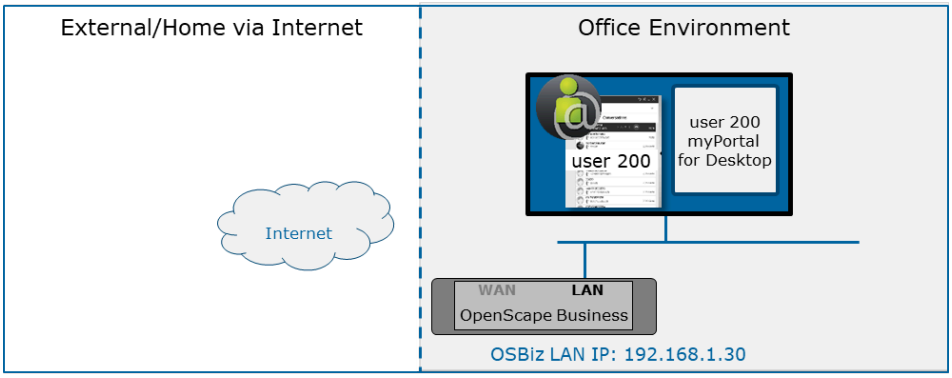
In order to use myPortal @work with user 200, the deskphone is automatically logged out and returns to the dummy number “100”. When switching back to deskphone again please ensure that myPortal @work is unregistered (# user must exit the application or log out).

Combination of myPortal @work with other UC Suite clients and license configuration

NOTICE: The configurations described in this chapter are also supported for home user via VPN.

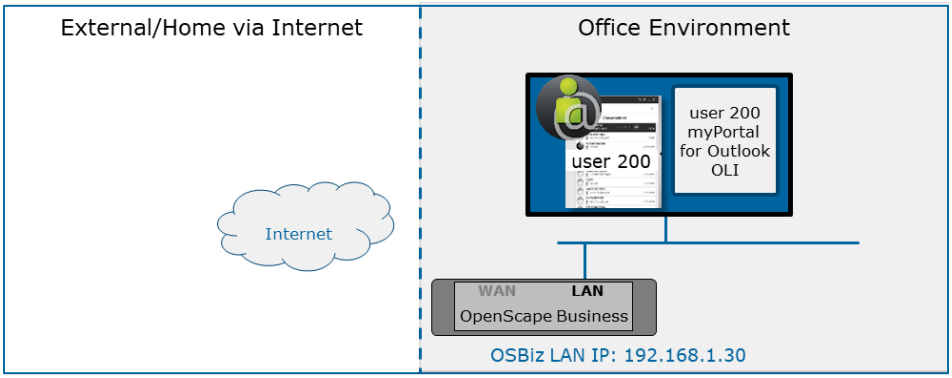
UC user license

The same user can be connected in parallel with myPortal @work and myPortal for Desktop.



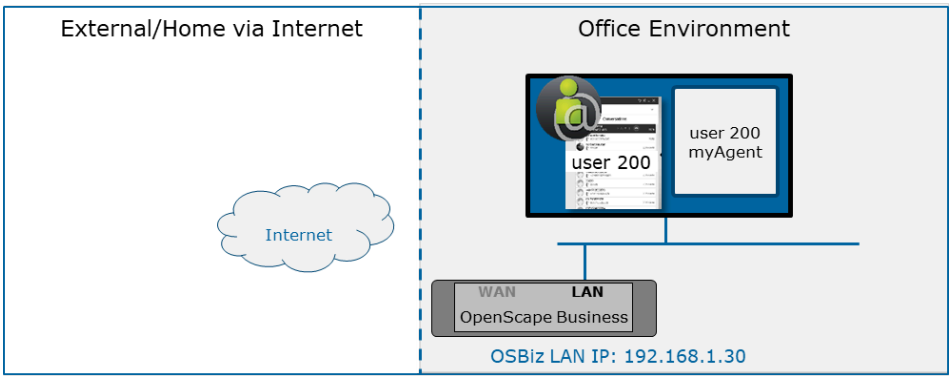
Groupware license

The same user can be connected in parallel with myPortal @work and OLI.



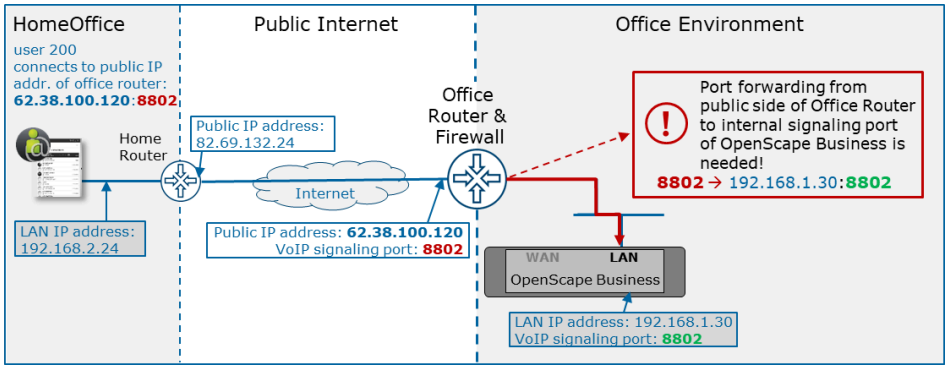
Combination of IP, UC user and myAgent license

myAgent and myPortal @work VoIP can be used as a softphone in parallel.



12.2.1.3 Configuration steps to use myPortal @work via the internet

In order to use myPortal @work from the internet the OpenScape Business therefore needs to be accessible from the internet as well. For all examples within this chapter, the following basic network scenario is assumed.



Network scenario description

The OpenScape Business is located within the office environment, which is connected to the internet via the office router. This router is accessible from the internet either via the public IP address of “62.38.100.120” or via a DNS name.

myPortal @work client is connected to the LAN within a home or external network, which is connected to the internet via a separated router. The external router is accessible from the internet with the public IP address “82.69.132.24”.

Configuration steps

To use the myPortal @work client on the OpenScape Business via the internet the following components need to be configured accordingly.

OpenScape Business within the office

Active STUN support on the system if not already done for an ITSP.

Configure myPortal @work user (SBC flag is not needed for VoIP)

Office router

Since myPortal @work client must reach the OpenScape Business from the internet and vice versa, the following configuration must be done on the office router to accomplish this:

- HTTPS port forwarding from the external port (default is 8802) to the internal port 8802 of the system
  - External port (default is 8802) -> Office Router -> 192.168.1.30:8802

For more information, see also chapter Ports and Firewall Settings on page 481

myPortal @work/ external router

The myPortal @work client needs to connect to the public IP address or DNS of the office internet router on the external port, which is by default 8802 (due to the previously configured port forwarding this will point to the OpenScape Business within the office network).

In most cases nothing additional needs to be configured on the external router but in case of a problem, see chapter Ports and Firewall Settings on page 481.

MULAP configurations

When a MULAP user is connected in UC Suite, it is not supported to run myPortal @work in two different devices simultaneously.

12.2.1.4 Other Configuration Hints & Settings

STUN server settings

For more information on how to configure the STUN server, see chapter "Configuring STUN" in guide “How to configure system device@home”and OpenScape Business V3, my Portal @work, User Guide section “How to add a STUN server”

Headsets

Every detected sound device / microphone found in the operating system can be used.

Jabra/Plantronics headset integration

In case of problems with Jabra headset integration, run the application with administrator rights.

In order to use Jabra headset integration, the Jabra device needs to be set as the main microphone device in myPortal @work.

For Plantronics integration, Plantronics hub should be installed.

Ports and Firewall Settings

Basically, the following ports must be configured for myPortal@work signaling:

- UC functionality & WebRTC / VoIP signaling: 8802
- Default STUN server port: 3478. If a custom STUN server is configured, a different port may be required.

Configuration of ports for WebRTC / VoIP payload depends on the type of firewall used in the customer environment. In order to run myPortal @work in a customer network environment it is fundamental to understand and check the type of used firewall, either stateful or stateless, and configure the firewall settings together with the responsible IT admin.

To better understand the differences between both type of firewalls please read the following:

- Stateless firewalls are designed to protect networks based on static information such as source and destination.
- A stateful firewall is a firewall that monitors the full state of active network connections. This means that stateful firewalls are constantly analyzing the complete context of traffic and data packets.

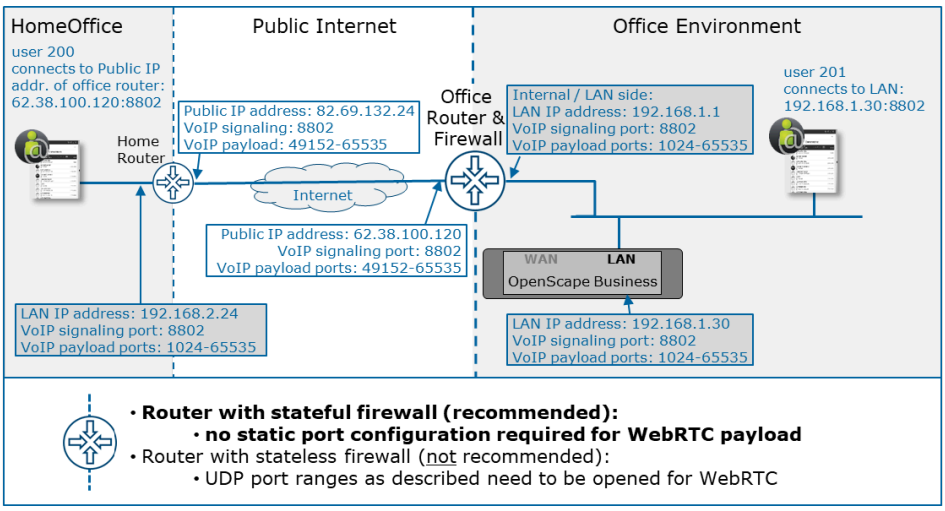
For further information on those firewall types please refer to the internet or relevant technical literature as a source of information.

It is assumed, that a stateful firewall/NAT device is going to be used in order to better protect private customer networks means that this device needs to allow internal outbound connections towards their destination.

The firewall/NAT device will block any packets in the inbound direction, unless it belongs to an already established session (on an ephemeral/dynamic port) which was previously established outbound.

In terms of the port usage nothing needs to be configured within the firewall/ NAT device since this will be handled and negotiated automatically when using a stateful firewall.

Using a stateful firewall is the recommended and more secured path to run WebRTC based VoIP solutions.



In terms of a stateless firewall (which is not going to be recommended for VoIP) the following range of UDP source ports for devices inside the customer network needs to be opened for internal payload traffic: 1024-65535.

For all payload traffic which is exchanged via the internet the WebRTC technology uses ports from the UDP port range of 49152-65535. For further information please refer to relevant technical literature as a source of information.

Each networking device on the path between the involved payload endpoints needs to be configured accordingly (e.g. router, firewall, NAT, proxy, etc).

Due to the broad port range which needs to be opened, stateless firewall cannot be recommend for VoIP.

Table 4:

	Stateful firewall	Stateless firewall to be opened statically
WebRTC / VoIP signaling port	8802	8802
WebRTC / VoIP payload UDP port range within local LAN i.e. within customer environment	dynamic[4]	1024-65535
WebRTC / VoIP payload UDP port range used over the public internet	dynamic[4]	49152-65535

[4] No configuration action needed; ports will be taken dynamically from same UDP port range as listed for stateless firewall

Restrictions on VoIP

- In scenarios with multiple calls (e.g transfer, conference, camp on) we recommend disabling the headset integration in case of an error. By deactivating the headset integration flag within myPortal @work only the headset's call control functionality cannot be used, but the headset can still be used as audio device.
- myAgent's "Free Seating" functionality (the agent can select the phone to be used via a drop-down menu during the logon process) i.e. free selection of a physical device by an agent is not supported in combination with myPortal @work.
- Symmetric NAT configuration is not supported.
- Strict firewalls are not supported.

12.2.1.5 Troubleshooting Guide

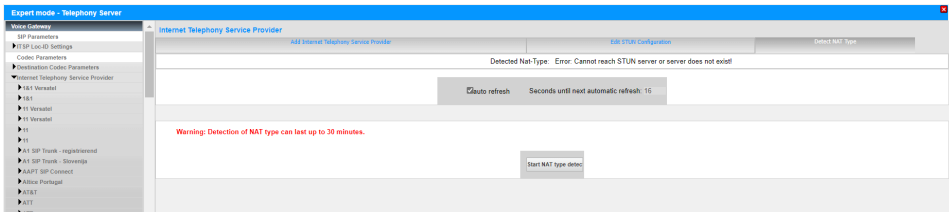
Connection Timeout

- As a home user with VPN connection, should ensure that the user can access the LAN address of the system and connect to the LAN address: 8802 port. Troubleshoot message: Error Message "connection time out", Action: check if the user when connected via VPN has a local IP from the VPN network.
- As a standalone user ensure that there is no other device or VoIP myPortal @work client registered with the same station number. Check also in **WBM > Expert Mode > Web Services Assistant** for the open connections.

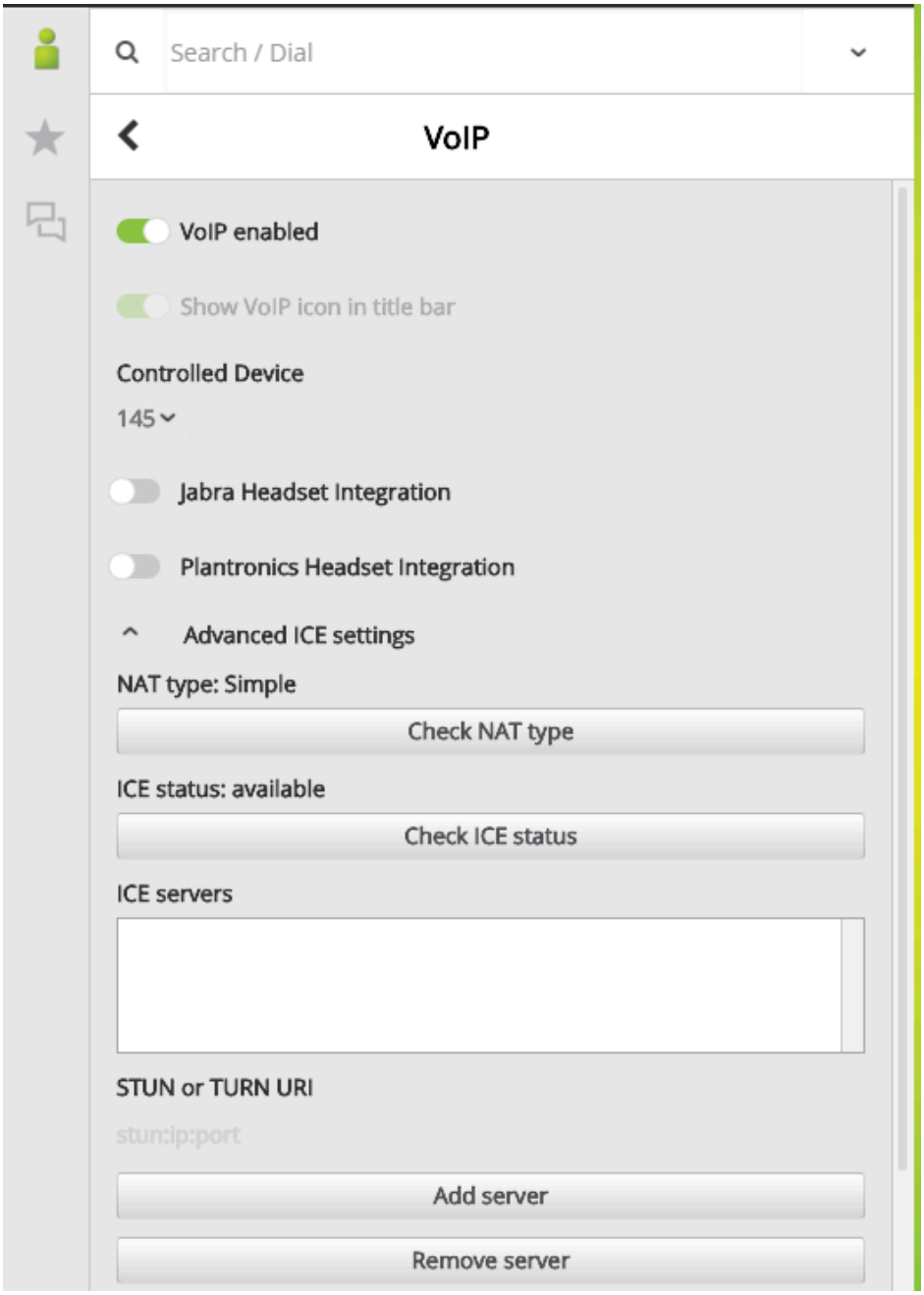
No Payload

In case of no payload permanent issue:

- Check that allowed ports are open on the firewall. For more information, see chapter Ports and Firewall Settings on page 481.
- Check NAT firewall configuration. Symmetric NAT configuration is not supported.
- You may detect NAT type from the system in **WBM > Expert mode > Voice Gateway > Detect NAT type**.
- Check STUN server connectivity in the system.



- Check ICE connectivity in myPortal @work: **Settings > VoIP > Advanced ICE settings**. In case "NAT type" and/or "ICE Status" are not as seen below, network/firewall settings need to be checked by your administrator.



Run “Check NAT type” > NAT type: Simple

Run “Check ICE status” > ICE status: available

- Disable headset integration from myPortal @work and perform the scenario again.
- Select again audio devices from VoIP settings.

12.2.1.6 Further Hints

SIP ALG (Application Layer Gateway)

If you experience one of the following issues, please check if a SIP ALG is activated on one of the involved routers. There are a few categories of symptoms SIP ALG could affect VoIP connections. It's not always apparent, especially since these issues often happen silently without users knowing.

- One-way audio (only one person can hear the other)
- Client does not ring when called
- Calls drop after being connected
- Calls going straight to voicemail for no known reason

12.3 Users of UC Smart

Users of UC Smart are subscribers who use the UC Clients of UC Smart.

The following settings for UC Smart clients are available in UC Smart Assistant:

Settings	Explanation
Settings	
Users	The setting is only displayed here.
Name	The setting is only displayed here.
Password	Password for UC Smart clients and UC Smart Assistant.
Language	Language of the user interface.
The user must assign a new password	The setting is only displayed here.
UC Smart Assistant access	User permission for the use of UC Smart Assistant in the web browser for configuration tasks.
Configured as Mobility stations	The setting is only displayed here.
Voicemail licence	The setting is only displayed here.
Associated Services	The setting is only displayed here.
Profile details	
Mobile phone number	Mobile phone number of the subscriber in canonical format (e.g., `+ 49 173 1234567`).
Private/External phone number	Additional phone number of the subscriber in canonical format (e.g., `+ 49 89 987654321`).
E-mail Address	E-mail address of the subscriber.
Voicemail to e-mail	Enable/disable the e-mail notification when a new voice message is received.
Presence visibility	Setting that determines whether the presence status is visible to both internal and external subscribers or just to internal subscribers or not visible to any subscribers.
Licence information	

Settings	Explanation
Display of licenses assigned to the user	

12.3.1 How to Configure UC Smart Users

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **UC Smart**.
3) Click on **Edit** to start the **UC Smart** wizard.
4) Click on **Administration** > **User Management** in the menu tree.
5) Select the desired user in the **Users** list.
6) Enter the data of the user in the **Settings** area and the **Profile Details** area.
7) Click **Apply**.
8) If you want to configure another user, repeat steps 5 through 7.

12.3.2 How to Change the Password for a UC Smart User

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

NOTICE: Please note that a UC Smart user must change his or her password again by default after the administrator has changed it. If this is not desired, the flag "User must change the password" must be disabled after changing the password.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **UC Smart**.
3) Click on **Edit** to start the **UC Smart** wizard.
4) Click on **Administration** > **User Management** in the menu tree.
5) Select the relevant user in the **Users** area.

NOTICE: A password, which consists of 5 stars (*****), will not be accepted by the system for security reasons.

6) Enter the new password under **Password** in the **Settings** area.
7) Click on **Apply**.

8) If you want to reset the password of another user, repeat steps 5 through 7.

Next steps

Notify the affected user(s) about the new password.

12.4 Presence Status (Presence)

The Presence status in the internal directory provides information on the availability of internal subscribers (including Mobility Entry stations). The Presence status also controls the availability of internal subscribers using status-based call forwarding.

As a subscriber, you can change your Presence status in myPortal @work or myPortal to go. For every change in the presence status (except for **Office**), you can also define the scheduled time of your return to the **Office** status if required.

As a subscriber, you can select the following statuses:

- **Office**
- **Meeting**
- **Sick**
- **Break**
- **Gone Out**
- **Vacation**
- **Lunch**
- **Gone Home**
- **Do Not Disturb**

NOTICE: The system administrator can enable/disable the visibility of status "sick" within the system administration. See OpenScape Business UC Suite > Server

---

Using the status-based call forwarding, calls can be forwarded to the personal voicemail box, for example. Subscribers who have no personal voicemail boxes can forward calls to a group mailbox or a system mailbox.

12.5 Directories and Journal

Directories and the Journal organize contacts and calls.

12.5.1 Directories

Directories are used to organize the contacts of subscribers. Subscribers can access these contacts with UC Smart clients.

The system provides the following directories, which support the following functions and with the below priority for lookup number (lookup number will be supported only for external call and in case that CO/ITSP does not provide the name):

Directory	UC Smart Clients	System telephone with a display
Personal directory	Outlook contacts imported via the Personal Assistant.	
Internal directory	Contains all internal subscribers and groups (with their phone numbers) for which the display has been activated in the system. Internal subscribers with system telephones are shown with presence status. The Presence status of a subscriber can only be shown if allowed by that subscriber.	Contains all internal subscribers and groups for which the display has been activated in the system.
Favorites list	Contains the contacts selected by the subscriber from his or her personal contacts and the internal directory. Internal subscribers with system telephones are shown with their respective presence statuses. The Presence status of a subscriber can only be shown if allowed by that subscriber.	
System Directory	Contains all central speed-dial numbers.	

NOTICE: Phone numbers in directories should always be entered in canonical format wherever possible.

NOTICE: When adding or removing a UC contact, it may take several minutes (**and** up to 30') until changes are applied on all clients and devices due to caching mechanisms that are used. Alternatively a system restart can be performed for the changes to take **immediate** effect.

12.5.1.1 How to Configure Directories for System Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile.

You can select which directories are to be made available on system telephones with displays.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **Display**.

4) Select one of the following options in the **Directory (phone book)** drop-down list:

- If all the personal contacts, the internal, external and networking directory and the LDAP directory are to be made available, select **All**.
- If only the personal contacts, the internal, external and networking directory is to be made available, select **Internal**.
- If only the LDAP directory is to be made available, select **LDAP**.
- If no directory is to be made available, select **No**.

NOTICE: The user can activated the search/lookup requests to be handled as requests to the Unified directory, by selecting the **Internal Phonebook via Unified Directory**. 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) Click **Apply**.

Next steps

If you have selected **All** or **LDAP**, make sure that an appropriate LDAP directory (e.g., Open Directory Service) is available for the system telephones.

12.5.2 Internal Directory

The internal directory contains the contact details of the internal subscribers and MULAP groups of the communication system. UC Smart clients can access the internal directory.

As an administrator, you have unrestricted access to all data in the internal directory. As a subscriber, you can dial from the internal directory.

The station parameter **Entry in telephone directory** (which can be set in the WBM via the Stations wizard) determines whether or not internal subscribers and groups are displayed in the internal directory.

In an internetwork, the internal directory applies across all nodes.

Related concepts

Group Call on page 653

12.5.2.1 How to Enable or Disable the Display of Stations in the Internal Directory

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Stations**.

3) Navigate in the menu tree under **Stations** > **Station** > **…** down to the desired station (Index - Station Number - Name).
4) Click on the **Edit Station Flags** tab.
5) Select one of the following options:
   - If you want the name of the subscriber to be displayed in the internal directory, enable the check box **Entry in telephone directory**.
   - If you do not want the name of the subscriber to be displayed in the internal directory, clear the **Entry in telephone directory** check box.
6) Click on **Apply**, followed by **OK**.

12.5.3 Favorites List

The Favorites list contains the contacts selected by the subscriber from the personal contacts and the internal directory. UC Smart clients have access to the Favorites list.

A UC Smart user can call a contact directly from the Favorites list. When an internal subscriber receives a call, the ringing state of the subscriber is displayed. The UC Smart user can then accept this call. In addition, the presence status for internal subscribers is displayed.

12.5.4 System Directory

The system directory contains all central speed-dial numbers for which a name was assigned. UC Smart clients can access the system directory.

The administrator individually disable the display for every subscriber and every speed-dial number with a name.

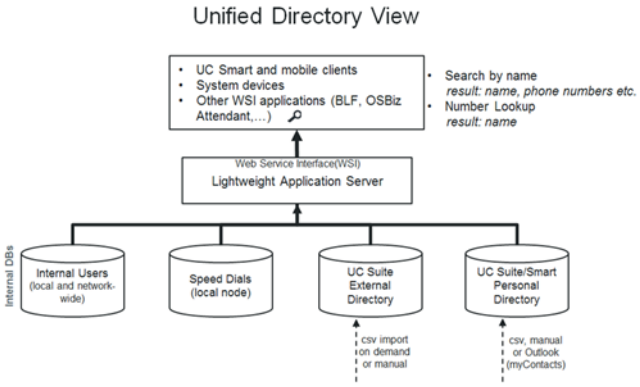
12.5.5 Unified Directory

OpenScape Business provides different data sources to store and to retrieve user or contact related data, starting with the internal user data in the internal user configuration, via the internal speed dial list, up to the different directories of the UC applications.

Each data source within OpenScape Business is used by a specific client application either located within the system SW itself in the phone devices or within a UC client application. Depending on the used data sources and the used clients, the retrieved data and their presentation is different.

The "Unified Directory" service within OpenScape Business comprises the existing OpenScape Business data sources for common search and name resolution functions. It provides the same search result or name resolution information to all system devices and OpenScape Business clients.

The Unified Directory service can either be accessed via the Web Service Interface (WSI) from externally located clients like myPortal to go or internally via the call processing mechanisms (e.g. from OpenStage Phones).



Unified Directory uses following internal databases and directories of OpenScape Business:

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

The Unified Directory service is available within every OpenScape Business system from V2R2 on. It does not require specific HW-SW or license prerequisites.

In order to get best results when using the Unified Directory some rules regarding phone number formats and writing of names have to be followed.

12.5.5.1 Features

Supported Devices / Clients

Unified Directory Service provides:

- Directory Search in several internal data sources of OpenScape Business
- Unified offering of the search result to all supported clients
- Phone number Look-Up / Name Resolution in several internal data sources
- Unified offering of name resolution results for all supported clients
- External data access via the WebServices Interface (WSI)

The features are available for single node systems as described in the following. Within OpenScape Business networks, the availability of the features depends mainly on the kind of connection of the trunks, devices and clients within the network.

Unified Directory supports following clients / system devices of Unify using the indicated interfaces:

Device/Client	Used Interface/ Protocol	Remarks
OpenStage phones	Call Processing / CorNet protocol	WSI / HTTP(S) is optional on OpenStage 60/80 for caller images

Device/Client	Used Interface/ Protocol	Remarks
OpenScape Deskphone IP	Call Processing / CorNet protocol	WSI / HTTP(S) is optional on DeskPhone IP 55 for caller images
Cordless (CMI) devices	Call Processing / CMI protocol	
CP 100/110 /200/205/210/ 405	Call Processing / CorNet protocol	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
Openscape Business Attendant/BLF	Call Processing / CorNet protocol	WSI / HTTP(S) is optional

NOTICE: The UC Suite myPortal, myAttendant and myAgent clients use their own mechanisms for directory search and name resolution.

Search function

The Unified Directory search is always performed by using the specific device / client user interface. The search criteria and the used character set could be restricted, depending on the used clients.

After the search criterion is entered the search is performed within subsequent directories

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

All matches within the directories above are shown as search results together with their origin. The matches contain either the full contact data set or only parts of it. The information depth of the results depends on the data source.

NOTICE: Group name search in myportal@work is not supported at UC Suite mode. Only licensed users (basic license) and licensed MULAP groups (UC Entries) search is supported.

The matches are presented at the devices or clients depending on display capabilities.

	Internal User Directory	Speed Dials	UC Smart Personal Directory	UC Suite External Directory	Personal Outlook Contacts (via my Contacts)
Last Name	X	---	X	X	X
First Name	X	---	X	X	X
Short/ Displayname	X	X	---	---	---
Office Phone No.	---	---	X	X	X
Home/Ext. PhoneNo.	---	---	X	---	X
Mobile Phone No.	---	---	X	X	X
Email-Adr.	---	---	X	X	X
Company name	---	---	X	X	X
City	---	---	---	---	---
Contact Picture	---	---	X	---	X
Contact Picturepreview	---	---	X	---	X

Phone Number Look-Up

Unified Directory Phone number Look-Up resolves the transferred calling party (CLI) by a number search in all supported internal data sources . The search is perfomed within following phone number fields:

- Office number
- Mobile number
- Home number

The Phone number Look-Up is triggered in case of incoming or outgoing calls in general, whereas specific routing and forwarding features are considered in addition.

A fixed prioritization of the data sources that are used for Phone number Look-Up is implemented in order to get the result as fast as possible. The result contains either only lastname, firstname, displayname or ,if available, the full related contact data.

Table 5: Supported Data Sources and Prioritization

Priority	Data Sources	Remark
1	CO/ITSP name (as sent by provider)	Prerequisite is to enable flag "Name in CO".
2	Speed dial list	
3	Personal Contacts	

Priority	Data Sources	Remark
4	UC User detail	

The retrieved data are presented on the user's device and/or in the UC client. The information depth depends on the display capabilities.

- **Incoming calls**

  Supported scenario for single node systems:

  – Basic call
  – Group call/ MULAP call
  – Ringing Group
  – Single Step Call Transfer (SSCT)
  – Attended/Supervised/Consultation Transfer
  – Call Forwarding Unconditional (CFU)
  – Call Forwarding No Reply (CFNR)
  – Call Forwarding Busy (CFB)
  – Blind transfer
  – Call Pickup

  NOTICE: Call Pickup is different from Call Pickup Group. In Call Pickup Group, when an external number is saved to the Unified Directory, the name of the caller is not shown from the members of the group.

  Supported scenario for multi node (network) scenarios is a Gateway Call.
- **Outgoing call**

  In case of an Outgoing Call the Phone number Look-Up of the called party number happens only once.

  Supported scenario for single node systems is a Basic Call to external number.

The presentation of the Phone number Look-Up result depends on display capabilities of the phones.

12.5.5.2 Rules and Conventions

Some conventions regarding number and name formats within the data sources have to be observed in order to get optimal results using the Unified Directory service.

Supported Number Format

All external phone numbers within the data sources must be entered in the canonical format including country and area code. e.g.+4989700712345

Speed Dial list supports only system dialable format e.g. 0089700712345 or 0004989700712345

When Speed Dial numbers are configured to be accessible through LDAP, you have to enable the Number conversion option to display the contact name when the number is in canonical format. For more information on how to enable

Number conversion, see How to Add an External Data Source for the Open Directory Service on page 1127.

Supported Name Formats

The following conventions regarding name formats and character sets have to be observed:

- **Speed dial name format**

  Name search within the Speed Dial List is supported only with specific configuration rules. The first and last names have to be entered within the existing name field using the following pattern:

  <Last Name>, <First Name> (comma separated)
- **Internal Users in case of Migrations**

  Migration to V2R1 and onwards with internal users that do not follow these configuration rules will not be supported in the expected way. This means the administrator should convert internal names to the following pattern before migration:

  <Last Name>, <First Name> (comma separated)

Availability of directory changes

After creating, updating or deleting contacts in the various data sources it can take up to 10 minutes until all changes appear on Phone number Look-Up results.

12.5.5.3 Functional Boundaries

The following functional boundaries do exist regarding Unified Direcrories:

Name Search

- Group name support

  Group names (not MULAP names) can not be searched in all kind of configurations
- Support of special characters

  On most phone devices the user can search for standard characters "a-z". Special (diacritical) characters like German characters Ää,Öö,Üü, ß are not accessible via phone device user interface.

  Therefore a plain character search result includes also special characters. A search for any of the characters "acdegilnorstuyz" matches with the corresponding special characters "àáâãåäąăäçćčďđèéêëęěğìíîïĺľłñńňòóôõöőřŕšśşťùúûůüűýÿžźż"

  in the search result.

NOTICE: Phonebook search with the wildcard character at the beginning of the search string, e.g. <*jo*>, is only supported for internal users.

- Support of Speed Dial Name format

  Name search within the Speed Dial List is supported only with specific configuration rules. The first- and last names have to be entered within the existing name field using one of the following patterns

  – <Last Name>, <First Name> (comma separated)
  – <First Name> <Last Name> (space separator on this case)

Name Presentation

Personal Contacts in UC Smart and from external offline directory, with length of first name plus length of last name greater than 24 characters, will be truncated to 24 characters length to fit the display length of the devices.

Phone number Look-up

The Phone number Look-Up feature (retrieve contact name from calling party number) is not supported in Unified Directory for SIP and S0 devices.

12.5.5.4 Unified Directory in Networked Systems

The Unified Directory Service is active within every node of an OpenScape Business Network and uses the datasources of the own system. Phone Devices and Client use always the Unified Directory Service within their own node.

Therefore it depends on the kind of datasource content if netwide contacts are available.

Table 6: Local and Netwide Datasource

Data source	Local data	Netwide data
Internal user directory	X	X
Speed dial lists	X	---
UC Smart Personal Directory	X	---
Personal Outlook Contacts (via myContacts)	X	---

NOTICE: The unified directory is not fully supported in mixed UC Suite/ UC Smart environments.

Phone number Look-up

In Networking scenarios the Phone number Look-Up functionality is not used. In such scenarios the name is transported via normal networking mechanisms between the network nodes.

For internal users the configured Display Name is used so Lookup is not required.

12.5.6 Journal

The journal is the list of all incoming and outgoing calls of a subscriber. It enables subscribers to quickly and easily respond to missed calls and call back their contacts or call them again directly from within the journal.

A maximum of the last 100 calls are displayed to UC Smart users.

Folder for Call Types

The calls can be arranged in the following groups:

- **Open**
- **Missed**
- **Accepted**
- **All Calls**

Call Details

Every call is shown with the Date and Time and, if available, with the call number. If a directory contains further details on the call number such as the **Last Name** and **First Name**, then this information is also shown. In addition, the **direction** and **duration** of the calls are displayed, as well as any redirections and call pickups that may have occurred.

12.6 Calls

For calls, the call number format is of particular importance.

12.6.1 Call Number Formats

Call numbers can be specified in different formats.

Format	Description	Example
Canonical	Begins with + and always includes the country code, area code and the full remaining station number. Blanks and the special characters + ( ) / - : ; are allowed.	+49 (89) 7007-98765
Dialable	Exactly as you would dial the call number on the system telephone in your office, always with the trunk access code.	• 321 (internal) • 0700798765 (own local network) • 0089700798765 (external local network) • 0004989700798765 (international)

INFO: If possible, you should always use the canonical call number format. This ensures that a phone number is always complete, unique and consistent for networking and mobile stations in every situation.

When dialing an external station (dialable format) manually, the CO access code must always be dialed as well.

When dialing an external phone number in dialable format from a directory (and when using the Desktop Dialer and Clipboard Dialer for certain UC clients), the communication system automatically adds the CO access code (route 1).

NOTICE: For calls within the USA via CSTA to a number in canonical format, phone numbers are converted to the dialable format.

12.6.2 Prerequisites for receiving VoIP calls on myPortal to go using CallKit on your iPhone

The iOS VoIP call notifications are based on Apple's APNS mechanism.

This service requires the following:

- A configured DNS server which resolves public domain names from the internet.
- Internet access for OpenScape Business system (port TCP/443 outbound) to send APNS call notifications.
- The system software needs to be up to date with the latest released major/minor/fix release. The latest system version is important because the APNS service requires specific certificates which expire when running older system software.

12.7 Conferences

In a conference, multiple participants (including external parties) can communicate with one another at the same time. The Conference Management function enables you to quickly and easily host conferences and also to schedule them in advance.

Phone-controlled and Application-controlled Conferences

As a subscriber, you can initiate conferences both via the phone and via the UC Smart applications.

You can initiate a phone-controlled conference in the following ways, and then control that conference via the phone:

- Call the desired conference participant and connect him or her to the conference
- Extend a consultation call into a conference
- Extend a second call into a conference

You can initiate, control and manage application-controlled conferences via the Conference Management. A Conference license is required for the use of Conference Management.

Differences between the conference types:

	Phone-controlled conference	Application-controlled conference
Direction of connection setup from the viewpoint of the system	• Outbound	• Inbound (dial-in by the participant)
Authentication of conference participants	-	• Personal PIN (conference ID) • Guest PIN (optional)
Predefined invitation to the conference participants	-	• Conference Name • Dial-in number (MeetMe) • Personal PIN (conference ID) • Guest PIN (optional)
Max. number of participants per conference	8	16

Scheduled Conference

Scheduled conferences are created as permanent conferences. The conference can be used as needed at any time without further scheduling. Scheduled conferences do not occupy any conference channel so long as no participant has dialed into the conference. The order of dialing in determines the assignment of the conference channels.

Administrators can change the specified dial-in number (MeetMe) for conferences via the WBM during the initial setup. The dial-in number with which the participants can dial into the conference is shown to the participants. They are then required authenticate themselves with their personal PIN or with the general guest PIN if allowed.

Moderators

The initiator of a conference is automatically the moderator and can:

- Create, edit and delete scheduled conferences.
- Add and remove conference participants.

  Removed participants do not remain in the conference.
- Disconnect conference participants.

  Disconnected participants can dial back into the conference.
- Specify another internal participant on the same node as the moderator
- Leave the conference without ending it immediately.

  If the last moderator leaves the conference, it ends after 5 minutes.
- End active conferences.
- Start a web collaboration session in an active conference.
- Send predefined invitations to all or individual conference participants.

All internal participants within a node can be moderators. However, a conference license is required for this.

Conference participants whose contact details were entered manually are treated as external participants and cannot be set as moderators.

Conference Participants

Conference participants can leave the conference and dial-in again. In addition, they can participate in a web collaboration session has already been started. As long as a conference has only one participant, the participant hears music on hold. The maximum number of external conference participants is limited, inter alia, by the number of available trunks.

Automatic Termination without a Moderator

If the last moderator leaves the conference, the other participants are notified with an info text that the conference will end after about 5 minutes.

Notification of Conference Participants

The moderator can send all or some conference participants an invitation by email. This requires an email program to have been installed on the client PC. Known email addresses are automatically added to the distribution list. In an invitation to all conference participants, only the general guest PIN (if allowed) is included; for individual invitations, the personal PIN is also sent.

Alternatively, a predefined invitation text can be copied to the clipboard for further use in other programs (e.g., a chat program).

12.8 Web Collaboration

myPortal supports the integration of the separate product Web Collaboration for simultaneous multi-media collaboration during phone calls and conferences. This provides quick access to functions such as desktop and application sharing, file sharing, co-browsing, whiteboarding, URL push, IM chat and video chat with multiple participants.

Web collaboration can be started by a subscriber during a phone call via the Call window of the UC PC client or by the moderator of an active conference from within the conference. A Web page from which the download of the web collaboration client can be initiated is opened. A local installation of Web Collaboration on the UC PC client is not required. If an email program is available on the UC PC client, an email with the link to the web collaboration client can be sent to the communication partners. Detailed information on web collaboration can be found in the Web Collaboration product documentation.

On deleting or ending a conference, the associated web collaboration session is automatically deleted as well.

Integration of Web Collaboration

In order to integrate web collaboration, the license number and password for the hosted web collaboration connection must be entered by the administrator in the WBM. The vendor offers the web collaboration server as a service on the Internet (Public Server). The license number and password are transmitted over a secure https connection. By default, TCP port 5100 is used for this purpose. Local web collaboration servers are not supported.

NOTICE: In order to use web collaboration, the UC PC clients and the communication system require an Internet

connection. Connections via a proxy are not supported by the communication system.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a web collaboration session are mutually independent, i.e., the instant messages from a UC PC client do not appear in a web collaboration session of the same participant, and vice versa.

12.8.1 How to Configure the Connection to the Web Collaboration Server (Public Server)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Internet access is available.

You need a license number and a password for the secure connection to the web collaboration server (public server).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Web Services**.
3) Navigate in the menu tree down to **Web Services** > **Web Collaboration**.
4) Select the **Public Server** radio button.
5) Enter the license number for the secure connection to the web collaboration server (public server) in the **Licence Number** field.
6) Enter the password for the secure connection to the web collaboration server (public server) in the **Password** field.

   NOTICE: If you want to test the Web Collaboration for 5 minutes, you can select the radio button **Public Server (Demo Mode/Evaluation Mode)**. No license number and password are required for this purpose.

7) Click on **Apply** followed by **OK**.

12.8.2 How to Disable the Connection to the Web Collaboration Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Web Services**.
3) Navigate in the menu tree down to **Web Services** > **Web Collaboration**.
4) Select the radio button **No Web Collaboration Server**.

5) Click on **Apply** followed by **OK**. The option to start a web collaboration session is disabled in the UC client.

12.9 Instant Messaging

Instant Messaging refers to communicating with instant messages (usually called a chat).

12.9.1 Instant Messaging

Using instant messaging, you can chat with other users of UC Smart.

The sent and received instant messages are presented to the communication partners as an interactive dialog. On selecting a recipient, the client shows whether the communication partner is currently online. If a communication partner is offline, no instant message can be transmitted to him or her. The IM overview page displays the most recent streams. The system stores a limited number of instant messages. A maximum of up to 100 of the last instant messages of a user are displayed.

12.10 Voicemail Box (SmartVM)

The voicemail box (also called SmartVM) plays a greeting to callers and offers them the option of recording a message or being routed to another number. Internal subscribers can access the voicemail box via a telephone and with the UC Smart client. Subscribers who want to use a voicemail box require a voicemail license.

Voicemail Box Types

The following different voicemail box types exist:

- Standard voicemail box:

  The standard voicemail box is the personal voicemail box of a subscriber. It accepts the call, greets the caller with a personal or standard announcement and offers the caller the option to leave a message. The standard voicemail box can be configured by the subscriber (by recording a personal greeting, for example) via the telephone or via UC Smart client.
- Group voicemail box:

  The group voicemail box has the same features as the standard voicemail box, except that it is not assigned to a single user, but a group of users. Messages can be recorded for a group voicemail box only if at least one member of the group has a voicemail license. The info of the voicemail box is displayed to all group members with a voicemail license. Message playback is possible through the phone menu of the personal voicemail box of the group members.
- Attendant voicemail boxes (AutoAttendant / Company AutoAttendant):

  The Attendant voicemail box offers callers a greeting with or without subsequent routing options. A special form of the AutoAttendant voicemail box is the Company AutoAttendant. Here, the caller can be optionally

forwarded automatically (to the switchboard, for example) or selectively to another station (e.g., to the service or hotline) by dialing an internal call number or speed dial number (digits 0-9). These dialing options must, of course, be explained with a corresponding announcement. It is also possible to configure an intercept destination to which the caller will be redirected if he or she fails to enter a digit or enters an invalid (i.e., unassigned) digit. The administrator can configure up to 100 Attendant voicemail boxes.

- Announcement voicemail box:

  The announcement function is configured by assigning an announcement index to an announcement port and configuring a voicemail box with the call number of the announcement port. The greeting of the mailbox is used as the announcement. Depending on the type of announcement, the playback may occur once (outgoing message) or cyclically (music). The phone menu of an announcement voicemail box can only be used from a different phone, since there is no associated phone. Consequently, a different PIN must be used for the announcement voicemail box than for the voicemail box of the used telephone.
- System voicemail box:

  The voicemail box with the call number of the hunt group of the SmartVM is used as a system voicemail box. The system voicemail box must be a standard voicemail box (not an AutoAttendant) with voice recording enabled. The info of the voicemail box is displayed to the owner of the voicemail box with index 1 and can also be checked from there. This first voicemail box should not be a Group, Attendant or Announcement voicemail box. If the system voicemail box is not to be used, then no voicemail box should be configured with the call number of the SmartVM hunt group.

Features of the Voicemail Box

- Checking and control via a telephone

  (from external location: own telephone number required)
- Manual or automatic selection of different greetings
- Phone menu (Telephone User Interface, TUI) with a system-wide switchable menu structure:
  - Phone menu, UC Smart: **SmartVM** (similar to EVM)
  - Phone menu, UC Suite: **OSO** (similar to UC Suite)
- Up to 320 voicemail boxes can be set up per system
- Up to 32 hours of voice recording capacity per system
- Up to 100 stored messages per voicemail box
- Up to 2 minutes of recording time for a voicemail per voicemail box
- Up to 10 simultaneously possible switching and call answering operations
- Announcement/music before answering
- Playback of individual announcements
- Forwarding of fax calls through automatic fax tone recognition to a preconfigured fax destination

---

NOTICE: Details on the phone menu can be found in the two Quick Reference Guides, UC Smart Telephone User Interface (TUI) and UC Suite Telephone User Interface (TUI).

Code Number Settings

Before the first use of the voicemail box, every subscriber must change the preassigned code number (default: `123456`).

The code number consists of a six digit sequence. Repeated digits (e.g., `333333`) and digit sequences in ascending or descending order (e.g., `987654`) are not allowed. After an invalid code number has been entered six times, access to the corresponding voicemail box is locked until the password is reset by the administrator. After two incorrect entries of the password via the phone menu, the connection is dropped.

Ports

The voicemail box uses the S_0 ports 500 to 509, which are assigned the call numbers 739 to 748, respectively. The ports 504 and 505 are assigned by default to the Company AutoAttendant (call number 352), and the remaining 8 ports are assigned to the voicemail box of the hunt group (call number 351). The call number 351 is the general call number of the voicemail box via which the phone menu is accessible.

Toll restriction

For security reasons, the ports of the voicemail box only have outward-restricted trunk access by default. The following features require the assignment of a COS group with direct trunk access:

- Call sender of a voice message
- Mobility users can listen to voice messages via callback
- Messages are transferred to an external destination using the Company AutoAttendant

Greetings / Announcements

Custom greetings (= announcements) can be either recorded from a phone or loaded into the system with the WBM. The configuration of a custom greeting via the phone occurs by dialing the voicemail box number and then using the user prompts of the voicemail box to record a new greeting over the phone.

Greetings can, however, also be loaded into the system separately for each voicemail box and subsequently saved or deleted in Expert mode.

NOTICE: For voicemail playback via external phone numbers (e.g. playback via mobile phone triggered by myPortal to go), the class-of-service of the Smart VM ports has to be adjusted. It is recommended to use an "allowed list" for such well-known numbers.

12.10.1 Configuring the Voicemail Box (SmartVM)

Configuring the voicemail box (SmartVM) includes the configuration of standard/group voicemail boxes and the Attendant voicemail boxes.

The general settings for the voicemail box (SmartVM) such as the adaptation of the voicemail box call number to a 4-digit dial plan, for example, are made via the **SmartVM** wizard.

The special settings for the voicemail box (SmartVM) and the setup of standard/ group voicemail boxes and Attendant voicemail boxes are performed in Expert mode.

NOTICE: Changing a call number resets the voicemail box of the corresponding subscriber. All personal voice messages, greetings and announcements are lost, and the password is reset.

You can also load individual greetings into the SmartVM, save and delete them, as well as back up and restore the greetings and messages of individual or all voicemail boxes. In addition you can check the loaded languages of the user prompts and display the 10 voicemail boxes with the most messages as well as the amount of storage space used by the messages and greetings.

The setup of Attendant voicemail boxes can be found in the section Attendants - AutoAttendants - Company AutoAttendant (UC Smart).

Assigning the Mailbox to Subscribers

Once the voicemail box (SmartVM) has been configured, the subscribers can be assigned their default mailboxes. This is possible through

- call forwarding for the subscriber with the aid of a call destination list (set up by the administrator). In this case, the call is forwarded sequentially to the selected call destinations (e.g., first to the subscriber and then - after a definable time period - to the mailbox).
- Call forwarding set up at the phone of the subscriber (which can be done by the subscribers themselves). In this case, the call goes immediately to the mailbox.

  If the subscriber is a member of a hunt group and the hunt group is called, the call is not redirected to the voicemail box of the hunt group.

12.10.1.1 How to Disable or Enable the Voicemail Box

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
3) Click on **Auxiliary Equipment** > **SmartVM** in the menu tree.
4) Click on the **Edit SmartVM Parameters** tab.
5) If you want to deactivate the voicemail box, select the **EVM Deactivation** check box.
6) If you want to activate the voicemail box, clear the **EVM Deactivation** check box.
7) Click on **Apply** followed by **OK**.

12.10.1.2 How to Configure the Voicemail Box (SmartVM)

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **SmartVM** wizard.
4) Select the **Activate SmartVM** check box.
5) If required, change the general settings for the system mailbox under the **Voicemail** column:
   a) If required, change the call number of the voicemail box in the **Call number** field (default: `351`) to adapt it to a 4-digit dial plan, for example.
   b) If required, change the direct inward dialing number of the voicemail box in the **DID** field (default: `351`) to adapt it to a 4-digit dial plan, for example.
   c) If required, change the name of the voicemail box in the **Name** field (default: `VOICEMAIL`).
6) If required, change the general settings for the Attendant mailbox under the **AutoAttendant** column:
   a) If required, change the call number of the voicemail box in the **Call number** field (default: `352`) to adapt it to a 4-digit dial plan, for example.
   b) If required, change the direct inward dialing number of the voicemail box in the **DID** field (default: `352`) to adapt it to a 4-digit dial plan, for example.
   c) If required, change the name of the AutoAttendant box in the **Name** field (default: `AutoAttendant`).
7) Click on **OK & Next**.
8) If required, change the call number of the port in the **Call no** field in the row of the desired port (default: `739-748`) to adapt to a 4-digit dial plan, for example.
9) If required, change the port name in the row of the desired port in the **Name** field (default: `SmartVM 1-10`).
10) If required, change the type of the port in the **Type** drop-down list in the row of the desired port.
    - **Phone mail (Callno. 5 digits)**: The port is assigned to the standard voicemail boxes and the Attendant voicemail boxes of type AutoAttendant. Ports of this type are automatically included in the hunt group 351.
    - **Standard**: The port is assigned to the Attendant voicemail boxes of type Company AutoAttendant and the announcement mailboxes. Ports of this type are automatically included in the hunt group 352.
11) If required, change the mode of the port in the **Mode** drop-down list in the row of the desired port.
    - **Announcement**: A greeting/announcement is played once.
    - **Music On Hold**: The greeting/announcement/music is played in a loop.
    - **Company AutoAttendant**: After playing a greeting/announcement, further switching is possible.

12) Click on **OK & Next**.
13) Select the desired mailbox in the **Mailbox selection** drop-down list. The fields for configuring the greetings will then appear.
14) If you want to use your own greetings for the selected mailbox, click on **Browse**, navigate to the storage location of the files (format: wave, PCM, 16 bit, 8 kHz, mono) and click on **Load**. The selected greetings are loaded into the system.

NOTICE: Previously loaded greetings can be saved or deleted.

---

15) If you want to set up greetings for further mailboxes, repeat steps 13 through 14.
16) Click on **OK & Next**.
17) You should change the general parameters only if required. For a description of the general parameters, see Auxiliary Equipment>SmartVM .
18) Click on **OK & Next** and then on **Finish**.

12.10.1.3 How to Add a Standard Voicemail Box for a Subscriber

Prerequisites

You are logged into the WBM with the **Expert** profile.

The corresponding subscriber has been assigned a voicemail license.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
3) Click on **Auxiliary Equipment** > **SmartVM** in the menu tree.
4) Click on the **Edit SmartVM Mailboxes** tab.
5) In the **Mailbox call no.** field, enter the call number of the subscriber for whom the voicemail box is to be added.
6) Select a greeting from the **Greeting** drop-down list.
7) If a caller may leave a message in the voicemail box, select the **Recording** check box.
8) Make sure that the **AutoAttendant** check box is selected.
9) The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.
10) Click on **Apply** followed by **OK**.

12.10.1.4 How to Change the COS Group for a Voicemail Box Port

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony Server** > **Classes of Service** in the navigation tree.
3) Click in the menu tree on **Classes of Service** > **Station** > **EVM** and then on the desired voicemail box port.
4) Select the desired COS groups for the day and night service on the **Edit COS Group** tab from the **Class of Service Group Day** and **Class of Service Group Night** drop-down lists, respectively.
5) Click on **Apply**, followed by **OK**.

NOTICE: EVM port texts are generated according to **Basic Configuration** wizard > **System Country Code**.

12.10.1.5 How to Change the Structure of the Phone Menu for the Voicemail Box

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
3) Click on **Auxiliary Equipment** > **SmartVM** in the menu tree.
4) Click on the **Edit SmartVM Parameters** tab.
5) If you want the structure of the phone menu to be similar to OpenScape Office, select the entry **OSO** in the **Telephone User Interface** drop-down list.
6) Click on **Apply** followed by **OK**.

12.10.1.6 How to Load, Save and Delete Individual Greetings

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Configuration** in the navigation tree.
3) Click in the menu tree on **Configuration** > **SmartVM Configuration** > **File Operations**.
4) Click on the **Greetings** tab.
5) Select the desired voicemail box from the **Mailbox selection** drop-down list.

6) If you want to load a previously saved greeting or a wave file into the SmartVM, click at the desired greeting on **Browse** and navigate to the storage location of the greeting. Then click **Load**.

NOTICE: The wave file to be loaded must have the following format: PCM, 8 kHz, 16 bit, mono. The wave file is converted on loading. Depending on the size of the wave file, this may take some time to complete.

---

7) If you want to save an existing greeting, click at the desired greeting on **Save** and save the vma file to a location of your choice.
8) If you want to delete an existing greeting, click at the desired greeting on **Delete** and confirm this with **OK**.

12.10.1.7 How to Back up and Restore Greetings and Messages

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Configuration** in the navigation tree.
3) Click in the menu tree on **Configuration** > **SmartVM Configuration** > **File Operations**.
4) If you want to back up greetings and messages:
   a) Click on the **Backup** tab.
   b) Select the **Messages** check box if the messages are to be backed up in addition to the greetings.
   c) Transfer the voicemail boxes to be backed up from the **Available Mailboxes** list to the **Mailboxes for backup** list.
   d) Click on **Apply**. The greetings (and messages if the **Messages** flag was enabled) of the voicemail boxes to be backed up are saved in a backup file (*.tar). Save the file to a location of your choice.
5) If you want to restore greetings and messages:
   a) Click on the **Restore** tab.
   b) Click on **Browse**, navigate to the storage location of your backup file (*.tar) and click on **Open**.
   c) Click on **Load** followed by **OK**. The voicemail boxes contained in the backup file are displayed.
   d) Transfer the voicemail boxes to be restored from the **Available Mailboxes** list to the **Mailboxes for restore** list.
   e) Select the **Messages** check box if not only the greetings of the selected voicemail boxes, but also the messages are to be restored.
   f) If the **Override** check box is cleared, only the greetings of the selected voicemail boxes that are present in the backup data will be overwritten. If the **Messages** check box is also selected, the messages contained in the backup data are included as well. The existing messages are retained
   g) If the **Override** check box is selected, all the greetings and messages of the selected voicemail boxes in the SmartVM will be deleted before the

restore. If voicemail boxes which are not contained in the backup data are selected, these will also be deleted! The greetings contained in the backup data are transferred. If the **Messages** check box is also selected, the messages contained in the backup data are transferred as well.

h) Click on **Load** followed by **OK**. The greetings and messages of the selected voicemail boxes are restored.

12.10.2 Notification Service for Messages

The system can optionally notify a UC Smart user about a new voicemail by e-mail.

Prerequisites for the Notification Service

- The delivery of e-mails (e-mail forwarding) has been configured by the administrator in the system.
- The user's e-mail address must be known to the system. The administrator can import all e-mail addresses in the WBM during the initial installation via an XML file or enter an e-mail address for each user in the UC Smart Assistant (see How to Configure UC Smart Users). Alternatively, users can specify their own e-mail addresses in their UC Smart client.
- A Voicemail licence is assigned to the user.
- The **Voicemail to e-mail** feature is enabled. The administrator can activate the feature for each user in the UC Smart Assistant (How to Enable or Disable E-mail Notifications). Alternatively, users can activate the feature themselves in their UC Smart client.

The UC Smart user receives an e-mail with the voicemail as an attached WAV file (16 bit, mono), together with the date and time of receipt, duration of the voicemail and, if available, the phone number and name of the sender.

12.10.2.1 How to Enable or Disable E-mail Notifications

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The **Package with UC Smart** has been activated under **Application Selection** in Expert mode.

The e-mail address of the user is entered in his or her profile details.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click on **Wizards** > **UC Smart**.

3) Click on **Edit** to start the **UC Smart** wizard.

4) Click on **Administration** > **User Management** in the menu tree.

5) Select the desired user in the **Users** list.

6) Select one of the following options:
   a) If you want to enable the notification service for new messages, select the**Voicemail to e-mail** check box in the **profile details** area.
   b) If you want to enable the notification service for new messages, clear the**Voicemail to e-mail** check box in the **profile details** area.
7) Click **Apply**.
8) If you want to configure another user, repeat steps 5 through 7.

13 UC Suite

The UC Suite provides unified communications features such as the Presence status and CallMe, conferencing, as well as voicemail, fax functionality and Attendant Console functions.

NOTICE: For the OpenScape Business hardware models X3/X5/X8, the UC solution UC Suite requires the UC Booster hardware (UC Booster Card or UC Booster Server). With OpenScape Business S (softswitch), the UC solution UC Suite is already integrated.

NOTICE: After changes in configuration of Stations, Groups, Mobility or other system parameters like trunk access codes, the UC Data for either UC Smart or UC Suite need to be synchronized. Synchronization occurs five minutes after the last configuration change. If a later configuration change occurs before the 5 minutes timer, the timer is restarted. UC Data may outdated until synchronization starts.

13.1 Basic Settings for UC Suite

The basic settings for UC Suite can be customized.

UC Suite can be enabled or disabled. If UC Suite is used, UC Smart must be disabled.

In addition, for all UC calls initiated by the system (e.g., via the Call-Me service), a check can be performed before dialing to determine whether the requesting UC user has the requisite class of service for that call. If the UC user does not have the required class of service, the call is not executed.

NOTICE: If CSTA applications are used, the code parameter for all active trunks should be set.

Related tasks

How to Determine the IP Addresses of the System Components on page 468

13.1.1 How to Activate UC Suite

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click in the navigation tree on **Applications** > **Web Services**.
3) In the menu tree, click on **Application Selection** > **Application Selection**.

4) Select one of the following options:
   - If you want to use the UC Suite with the UC Booster Card, click on **Package with UC Suite**.
   - If want to use the UC Suite with the UC Booster Server, click on **Package with UC Suite on OSBiz UC Booster Server** and, in addition, enter the IP address of the external Linux server in the **IP address of the OSBiz UC Booster Server** field.
5) Click on **Apply**.

13.1.2 How to Restrict the Authorization for UC Calls Initiated by the System

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click in the navigation tree on **Telephony Server** > **Basic Settings**.
3) In the menu tree, click **Basic Settings** > **System** > **System Flags**.
4) If an authorization check before dialing is to be performed for system-initiated UC calls to verify whether the requesting UC Suite user has the required class of service for that call, select the **Restriction for UC calls** check box in the **Restriction for UC calls** area.
5) If no authorization check before dialing is to be performed for system-initiated UC calls to verify whether the requesting UC Suite user has the required class of service for that call, clear the **Restriction for UC calls** check box in the **Restriction for UC calls** area.
6) Click on **Apply**.

13.2 UC Suite Clients

UC Suite clients provide subscribers with convenient user interfaces for comprehensive unified communications functions.

The system offers the following UC Suite clients for the following devices:

Client type	Client	Device
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	myPortal @work	
	Fax Printer	
	myAttendant	
Mobile Client	myPortal to go (UC Suite) (see Mobility)	Smartphone, Tablet PC

Client type	Client	Device
Contact Center Client	myAgent (see Multimedia Contact Center)	PC
	myReports (see Multimedia Contact Center)	

Subscribers with a configured e-mail address receive a welcome e-mail with Getting Started instructions.

Custom Settings

The custom (i.e., subscriber-specific) settings for myPortal for Desktop are stored in ini files on the PC. A separate ini file is created for every user. The custom settings for myPortal for Outlook, myAttendant and Fax Printer are stored in the registry of the PC. This enables different users to use the myPortal for Desktop, myPortal for Outlook, myAttendant and Fax Printer applications on a single PC (Desk Sharing) and also the deployment in Windows Terminal Server and Citrix Server environments. This allows different users to access the applications from their PCs without a local installation.

13.2.1 myPortal for Desktop

myPortal for Desktop is a client for unified communications on your PC. Besides convenient dialing aids via phone directories and favorites and information on the presence status of other subscribers, users can, for example, also access their voicemails and fax messages.

myPortal for Desktop provides the following features:

- Directories
- Favorites List
- Journal
- Desktop Dialer
- Screen Pops
- Presence status
- CallMe service with ONS (One Number Service)
- Status-based call forwarding
- Personal AutoAttendant
- Conference management
- Recording conferences
- Record calls
- Instant Messaging
- Voice and fax messages

13.2.2 myPortal @work

myPortal @work is a Unified Communication application, which combines all needed features and services, like convenient dialing via phone directories, favorites, conversations and information on the presence status of colleagues,

into a single solution design to accelerate daily communication, improve teamwork and to get in quick contact with colleagues, customers and partners.

Only one session at a time with myPortal @work, is allowed with the same user.

NOTICE: When myPortal @work VoIP client is used in combination with other UC Suite clients, it is recommended to use consultation hold, instead of common hold.

myPortal @work can be used with both UC Smart and UC Suite solutions. For more information, see myPortal @work User Guide.

13.2.3 myPortal for Outlook

myPortal for Outlook is the client for unified communications in Microsoft Outlook (plug-in) and is analogous to myPortal for Desktop.

myPortal for Outlook provides the following features in addition to those of myPortal for Desktop:

- How to Call an Outlook Contact
- How to Create an Outlook Contact from the Sender of a Voice Message
- How to Send a Voice Message as an E-mail
- How to Send a Fax Message as an E-mail

13.2.4 Fax Printer

Fax Printer is a Windows application for sending fax messages with individually created cover sheets from other Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax Printer Driver - with the following features:
  - Sending faxes to individual recipients
  - Directories
  - Use of central cover sheets
  - Using predefined headers
  - Merge fax
  - Control via the user interface
  - Control via the command line

13.2.5 myAttendant

myAttendant is a unified communications solution for Attendant functions. Besides convenient Attendant functions, dialing aids via phone directories and information on the presence status of other subscribers, myAttendant can, for example, also be used to access voicemails and faxes. Instant Messaging supports the communication with internal subscribers.

myAttendant provides the following features:

- Attendant functions
- Directories
- Journal
- Pop-up windows
- Change the presence status of subscribers
- Record calls
- Message Center
- User Buttons
- Manage voice and fax messages
- Instant Messaging
- Team functions
- Conference management

13.2.6 Prerequisites for UC Suite PC Clients

To use UC Suite PC clients, the client PC must be equipped with the appropriate hardware and software configurations. Depending on the configuration, administrator rights are required for the installation and automatic updates. The available functionality depends on the licenses being used.

NOTICE: Please make sure that you refer to the current notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Telephones

The UC clients can be used in combination with the following telephones:

- OpenStage HFA and SIP
- OpenScape Desk Phone IP 35G/55G HFA and SIP
- OpenScape Desk Phone IP 35G Eco HFA and SIP
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA and SIP
- OpenScape Desk Phone CP 110/210/410/710 HFA and SIP
- SIP phones with 3PCC support
- Analog telephones
- ISDN Phones
- OpenScape Personal Edition HFA and SIP
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Older devices (such as optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 and optiPoint WL2 SIP) are supported. Optiset E devices cannot be operated. For details on the tested and released devices, please refer to the Release Notice.

NOTICE: OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrated Client does not have any special prerequisites, apart from the standard client configuration and license.

"Favorites" in phone menu contains Free Programmable Keys and does not relate to UC Favorites. Details for those keys and how to, are available within the device documentation.

NOTICE: For analog and DECT telephones, the Message Waiting Indication (MWI) is not supported, and only limited support is available for displaying information on the phone.

Operating Systems

The UC Suite PC clients can be used in conjunction with the following operating systems:

- Microsoft Windows 11 (64 Bit) all versions
- Microsoft Windows 10 (64 Bit) all versions
- Apple macOS 13 / 14 / 15.1 to 15.4

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for the UC Suite PC clients for Microsoft Office 2003, Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Local administrator rights on a client PC are required for the installation under Windows, but not for automatic updates. The Russian and Chinese user interfaces of myPortal for Outlook require a corresponding Russian or Chinese Windows installation.

myPortal for desktop for Apple MAC is available with same interface as under Microsoft Windows. However, due to the Apple MAC OS system architecture, the following functions are currently not supported:

- Sending faxes
- Outlook, Entourage Integration

myPortal for Outlook is supported in Microsoft Office 365 environments. Microsoft Office 365 is a cloud application It includes, among other things, an Exchange server for the centralized distribution of e-mails as well as the traditional Microsoft Office products. OpenScape Business supports Microsoft Office 365.

The following functions can be used under Microsoft Office 365:

- Exchange Calendar Integration
- E-Mail Forwarding

Web Browsers

The following web browsers have been released for programming telephone keys via the UC clients:

- Microsoft Internet Explorer Version 10 (or later)
- Microsoft Edge
- Mozilla Firefox Version 19 (or later)
- Google Chrome

Additional Software

Additional Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java JRE 1.8.x or above (32 bit / 64 bit) OpenJDK V8 or above (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) - supported, but not part of the system test anymore - in case of error no SW correction will be delivered (end of sustaining by OpenScape Business)			X
Access to Microsoft Exchange Server (for Outlook contacts and appointments) Exchange 2015 / 2013 / 2010 (64 Bit)	X		X
Microsoft .NET Framework >= 4.0 (as of Outlook 2010)			X

NOTICE: To use the Exchange Calendar integration with Microsoft Small Business Server, FBA (Form Based Authentication) may need to be disabled there under some circumstances.

Note about Java 32 bit or 64 bit

To use the myPortal for Desktop function "Import Outlook Contacts at Startup" in conjunction with the 64-bit version of Microsoft Office 2013, an installation of the 64-bit variant of Java is required. If this function is not used, the Java 32 bit version is recommended, since the memory requirements for it are significantly lower. For this reason, the 32-bit version of Oracle Java or OpenJDK is generally recommended for all other installations as well.

NOTICE: Continuous use of the existing Oracle Java with OpenScape Business does not require any change. If a change of the Java version is required (for example upgrade from Oracle Java 7 to Oracle Java 8 or to Open JDK V8) then a reinstallation of the communication client is required.

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN (1 Gbps LAN recommended)
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

NOTICE: 4K monitors are not supported for myPortal and myAttendant.

Microsoft Terminal Server, Citrix XenApp Server

The UC Suite PC clients can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

INFO: Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

INFO: Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows 2022 Server 64 Bit
- Microsoft Windows 2019 Server 64 Bit
- Microsoft Windows 2016 Server 64 Bit
- Microsoft Windows 2025 Server 64 Bit

Office applications:

Microsoft Outlook / Office

- 2021 (32 bit / 64 Bit) + Office 365
- 2019 (32 bit / 64 Bit)
- 2016 (32 bit / 64 Bit) - supported, but not part of the system test anymore - in case of error no SW correction will be delivered (end of sustaining by OpenScape Business)

Hardware Prerequisites:

The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the Service The administrator can download the installation files from the **Service Center** and provide them to the users via a network drive, for example.
- The administrator downloads also the offline installer repository from example.
- The administrator can also download the offline installer repository from the **Service Center** and the clients can be installed offline.

13.2.7 Silent Installation/Uninstallation for UC Suite PC Clients

Silent installation/uninstallation is a command-line based method to automatically install, uninstall or modify UC Suite PC clients on a PC without requiring any further user inputs.

NOTICE: Please make sure that you refer to the notes in the `ReadMe first.rtf` file.

The silent installation/uninstallation requires local administration rights on the relevant PC. The silent installation/uninstallation process can also be logged in a file.

The following parameters are available for silent installations / uninstallations:

Parameters	Components
`/quiet`	Starts the installation procedure without user intervention and without a user interface. This parameter requires that the repository is already found.
`/repository`	Sets the IP address or the hostname to use during installation. For example, `/repository=192.168.50.50`
`/installpath`	Sets the path of the installed clients. The default value is: `C:\Program Files(x86)\communicationsclients\`
`/autostart`	Starts the installation procedure without user intervention. This parameter requires that the repository is already found.
`/i`	Selects a product to be installed. Available values are `OLI`, `myPortal`, `myAgent`, `FPD`, `myReports` and `all`. For example: `/i="OLI,FPD"`
`/u`	Selects a product to be removed. For example: `/u="OLI,FPD"`
`/set`	Selects the products that should be installed in the system. This switch will install the selected products, or modify them if they are already installed. It will also remove installed products that are not listed in the provided set. For example: `/set="OLI,FPD"`
`/repair`	Repairs the specified products. For example: `/repair="OLI,FPD"`

13.2.7.1 How to Perform a Silent Installation

Prerequisites

Your PC meets the requirements described under Prerequisites for UC Suite PC Clients.

You have local administration rights on the client PC.

The file `CommunicationsClients.exe` is available on the client PC.

NOTICE: Please make sure that you refer to the notes in the `ReadMe first` file.

Use the command line in accordance with the following patterns in a batch file or in a window with the DOS command prompt.

Step by Step

1) If you do not want to log the process, execute the following command:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i=all /quiet
   ```

   Where `<IP-address>` must be replaced with the IP of UC Clients.

2) If you want to log the process in a file, for example, in `C:\ccinstall.log`, execute the following command:

   ```
   CommunicationsClients.exe /repository=<IP-address> /
   i="myPortal,FPD" /quiet /l="C:\ccinstall.log"
   ```

   Where `<IP-address>` must be replaced with the IP of UC Clients. The above command installs only myPortal for Desktop and FaxPrinter. You can modify it to install the clients you want.

13.2.7.2 How to Perform a Silent Uninstallation

Prerequisites

Your PC meets the requirements described under Prerequisites for UC Suite PC Clients.

You have local administration rights on the client PC.

The file `CommunicationsClients.exe` is available on the client PC.

NOTICE: Please make sure that you refer to the notes in the `ReadMe first` file.

Use the command line in accordance with the following patterns in a batch file or in a window with the DOS command prompt.

Step by Step

1) If a system update was performed after the last silent installation, repeat exactly the same command line with the new `CommunicationsClients.exe` file as was done with the earlier `CommunicationsClients.exe` file (i.e., as if you wanted to reinstall the components installed earlier with the new `CommunicationsClients.exe` file. It is only then that a silent uninstallation will be possible.

2) If you do not want to log the process, select one of the following command lines:

   - If you want to uninstall all the components:

     ```
     CommunicationsClients.exe /quiet /u=all
     ```
   - If you want to uninstall multiple components, specify their corresponding parameters as a comma-separated list after `/u=`, for example, myPortal for Desktop / myAttendant and Fax Printer:

     ```
     CommunicationsClients.exe /quiet /u="myPortal,FPD"
     ```
   - If you want to uninstall only one component, enter the appropriate parameter after `/u=`, for example, myPortal for Desktop / myAttendant:

     ```
     CommunicationsClients.exe /quiet /u=myPortal
     ```

3) If you want to log the process in a file, e.g., in `C:\ccuninstall.log`, select one of the following command lines:

   - If you want to uninstall all the components:

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u=all
     ```
   - If you want to uninstall multiple components, specify their corresponding parameters as a comma-separated list after `/u=`, for example, myPortal for Desktop / myAttendant and Fax Printer:

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u="myPortal,FPD"
     ```
   - If you want to uninstall only one component, enter the appropriate parameter after `/u=`, for example, myPortal for Desktop / myAttendant:

     ```
     CommunicationsClients.exe /quiet /l="C:
     \ccuninstall.log" /u=myPortal
     ```

13.2.8 Automatic Updates

Automatic updates ensure that the UC clients are always kept up-to-date with the latest version.

If a new version is available, the update will either be installed automatically or you will be notified that an update is available. If necessary, a message is displayed indicating that one or more applications must be closed to perform the update.

NOTICE: We recommend that you always perform the updates offered. This also applies to software that is required for certain UC clients.

NOTICE: Automatic update of myPortal @work is not supported in MacOS.

13.3 Users and User Profiles of the UC Suite

Users of UC Suite are the subscribers who use the UC clients of UC Suite. User profiles store the settings of the users of UC Suite.

13.3.1 Users of UC Suite

UC Suite users use the UC clients of UC Suite. The settings of the UC Suite users are configurable in the user directory.

The user directory contains all the subscribers in the system. In order to use the UC clients, additional user data must be configured in the user directory.

The following information is displayed in the user directory for every user:

- Symbol for presence status

  The administrator can change the presence status for every user.
- **Extension**
- **User name**

  NOTICE: While UCSuite does allow and support the change of usernames for its own clients, nevertheless such changes could affect the login of non-UCSuite clients like myPortalToGo/myPortal@Work (where applicable), hence not recommended in such situations.
- **Name**

  First and last name, as configured for the subscriber.
- **Department**

  If a department is assigned to the user.
- **E-mail**

  E-mail address
- **Is Agent**

  Agent level for Multimedia Contact Center.
- **Voicemail**

  The user can receive voicemail.
- **Call Forwarding**

  Call forwarding is configured for the user.

Search functionality is also available for the user directory fields.

The following settings can be configured:

Values and settings	Keywords
Personal details	
My Personal Details	Own name, user name, password, e-mail address, department, additional phone number

Values and settings	Keywords
My Picture	My Picture Supported file formats: BMP, JPG/JPEG/JFIFI, PNG. Maximum file size: 10MB
User Level	Receiving voicemails: see Stations User as Attendant Console: see Stations User as agent: see Stations
My Preferences	
Presentation	Skin colors, language of the user interface
Notifications	Screen Pops
Calendar connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook/iCal appointments
Hotkeys	Hotkey for functions
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address, function keys of the telephone
Call Rules	
Forwarding destinations	Status-based Call Forwarding
Rules Engine	Rule-Based Call Forwarding
Communications	
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
Profiles	
Busy, No Answer, Meeting, Sick, Break, Away, Vacation, Lunch, Home Ph.	profile for personal AutoAttendant
Sensitivity	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers
Allow other users to copy my BLF layout	Allow other users to copy the BLF groups and buttons This option is not available for the profiles that have already been created.

Values and settings	Keywords
myAttendant	
LAN Messages	Text module for Instant Messaging
DIDs	MSN
Communications	Call forwardings

Additional information on user settings can be found in the User Guides of the UC clients and under the keywords listed in the table.

The password for UC clients consists of six digits by default. The password length can be adapted as required (6-10 characters). The maximum number of repeated characters is two and the maximum number of sequential characters is three. The account name (reversed or not) cannot be part of the password and the password change requires knowledge of the old password. The user is forced to change the default password after the first use. The maximum number of erroneous login attempts is five. An administrator with the **Advanced** profile can change the password of a user (if the user has forgotten it, for example).

NOTICE: The First Name and Last Name of a user are overwritten in the User Directory when they are changed by using a wizard or in Expert mode. By contrast, if the First Name and Last Name of a user are changed in the User Directory, the user data displayed when using a wizard or in Expert mode are not overwritten. This results in the existence of two different user names for the same user. Additionally, if the length of first name and the length of last name is greater than 16 characters in total, then it will be truncated to 16 in order to fit to dispay of the device.

Subscribers for whom an e-mail address has been configured and who use myPortal for Desktop receive a welcome e-mail with Getting Started Instructions.

Resetting User Data

The settings of a user can be reset to default values. Resetting user data will delete all user's data, including First Name, Last Name and Login Name.

Whether or not the user has First or Last Name set via **WBM** > **Expert Mode** > **Telephony Server** > **Station**, resetting this user via UC Suite will eventually assign the number that is stored as Extension also in the **Name** field.

13.3.1.1 How to Configure UC Suite Users

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click on **Edit** to start the **User Directory** wizard. All users are displayed.
4) Mark the desired user and click **Edit**.
5) Edit the data of the user.
6) Click on **Save**. The window is automatically closed. All users are displayed.
7) If you want to configure another user, repeat steps 4 through 6.

13.3.1.2 How to Reset UC Suite Users

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard. All users are displayed.
4) Mark the desired user and click **Reset User**.
5) Click on **Save**. The window is automatically closed. All users are displayed.
6) If you want to reset another user, repeat steps 4 through 5.

13.3.1.3 How to Configure UC Suite Users as Agents (myAgent)

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard. All users are displayed.
4) Click in the row with the relevant user.
5) Click **Edit**.
6) Click on **Personal Details** > **User Level**.
7) Select one of the following options:

   If the agent is to be permanently available, select the **Permanently available agent** check box. The agent will then remain available for calls, faxes and e-mails even when he or she does not accept a call, fax or e-mail.

   If the agent is not to be permanently available, clear the **Permanently available agent** check box. The agent will then be assigned the status Unavailable when he or she does not accept a call, fax or e-mail.
8) In the **Level** drop-down list, select the desired role for this agent: **Agent**, **Supervisor** or **Administrator**.
9) Click **Save**.
10) If you want to configure another user as an agent, repeat steps 4 through 9.

13.3.1.4 How to Change the Presence Status for a UC Suite User

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard. All users are displayed.
4) Select the desired user.
5) Click on the presence status icon and select the relevant presence status from the drop-down list. If necessary, enter the time of return in the format `yyyy/mm/dd hh:mm`, e.g., `2012/12/12 12:00`.
6) Click on **Save**.
7) If you want to change the presence status for another user, repeat steps 4 through 6.
8) Close the window.

13.3.1.5 How to Change the Password for a UC Suite User

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard. All users are displayed.
4) Mark the corresponding user and click **Edit** > **Personal Details** > **My Personal Details**.
5) Under **Password**, click on **Change**.
6) Enter the new password under **New**.
7) Enter the new password under **Confirm**.
8) Click on **OK**. The window is automatically closed. All users are displayed.
9) If you want to change the password of another user, repeat steps 4 through 8.

Next steps

Notify the affected user(s) about the new password.

13.3.1.6 How to Change the Password Length for UC Suite Users

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **General Settings**.
5) Enter the minimum required password length (6-10) for the future in the **Lengths** field, under the**Length of Password** area.
6) Click on **Save**.

13.3.2 User Profiles for the UC Suite

User profiles of the UC Suite store the settings of the UC Suite users. One or more users (members) can be assigned to a user profile. All members of this profile have the same settings.

Every user can be a member of no more than one user profile. Direct changes to the settings of a user - i.e., not via the assigned profile - automatically delete the user from the profile.

If a user is unassigned from a profile they retain the settings that are represented by this profile.

When a user is already assigned to a profile, only changes in the locked profile items will be applied to that user. If the lock symbol is unlocked, then the changes will not apply.

If an entire profile is deleted,users that were assigned to this profile also retain profile's settings.

The following values and settings can be configured:

Menu items	Values and settings for
Personal details	
My Personal Details	Visibility of phone numbers
My Preferences	
Appearance	Skin colors, language of the user interface
Notifications	Screen pops
Outlook connectivity	Automatic creation of Outlook appointments when absent, automatic update of presence status via Outlook/iCal appointments
Hot Keys	Activation and set up of key combinations for access to various commonly used functions through the keyboard. The lock symbol determines whether users can change these settings themselves.
Miscellaneous	Automatic reset of the presence status, transfer method, retention period for Journal entries, server address

Menu items	Values and settings for
Call Rules	
Forwarding destinations	Status-based call forwarding
Communications	
Voicemail settings	Recording or announcement mode, language of the voicemail box
VM Notification	Notification Service for Messages
Fax Notification	Notification Service for Messages
Missed Call Notifications	Notification Service for Missed Calls
VoiceMail Profiles	
VoiceMail Profiles	Profile for personal AutoAttendant. Available status: Busy, No Answer, Meeting, Sick, Break, Out of Office, Holiday, Lunch, Home
Sensitivity	
Security and Access	Retrieval of your voice and fax messages by the Attendant; password check for the voicemail box
Presence Visibility	Visibility of your Presence Status for Others
VoiceMail Presence	Announcement of your presence status for external callers; announcement of your presence status for specific callers
Favorites	
Favorites	Favorite groups with a list of contacts that can be assigned to the user.

Additional information on user profile settings can be found in the User Guides of the UC clients and under the keywords listed in the table.

13.3.2.1 How to Add a UC Suite User Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All user profiles and their members are displayed.
4) Click on **Add**.
5) Enter the desired name for the profile under **Name**.
6) Click on **Save**.
7) Configure the desired settings for the user profile.

8) Click on **Save** and close the window.

13.3.2.2 How to Edit a User Profile of the UC Suite

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All profiles and their users are displayed.
4) Select the desired profile.
5) Click on **Edit**.
6) Change the desired values and settings.

NOTICE: Click on **Save** before you switch to a different menu item so that your changes are applied.

---

7) Then click **Save** and close the window.

13.3.2.3 How to Display the User Profiles of the UC Suite

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All user profiles and their members are displayed.

13.3.2.4 How to Add Members to a UC Suite User Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All user profiles and their members are displayed.
4) Select the desired user profile and click **Assign Users**.
5) Select the desired members from the **Available Users** list.

6) Click on **<-** to transfer them to the **Assigned Users** list.

   All station profiles and their members are displayed.
7) Close the window.

13.3.2.5 How to Delete Members from a UC Suite User Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All user profiles and their members are displayed.
4) Select the desired user profile and click **Assign Users**.
5) Select the relevant members from the **Assigned Users** list.
6) Click on **->** transfer them to the **Available Users** list.

   All station profiles and their members are displayed.
7) Close the window.

13.3.2.6 How to Delete a UC Suite User Profile

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Profiles** wizard. All user profiles and their members are displayed.
4) Select the desired user profile.
5) Click on **Remove**.
6) Click **OK** to confirm your selection. All station profiles and their members are displayed.
7) Close the window.

13.4 Presence Status and CallMe Service

The Presence status and CallMe service display and optimize the availability of subscribers. The Presence status enables simple status-based call forwarding as well as rule-based call forwarding, which can be flexibly configured with myPortal for Desktop or myPortal for Outlook.

13.4.1 Presence Status (Presence)

The Presence status indicates the availability of internal subscribers (including mobile stations) in the Favorites list, the internal directory, the virtual conference room and via voicemail announcements. In addition, the Presence status controls the availability of internal subscribers with status-based call forwarding, rule-based call forwarding and the personal AutoAttendant.

As a subscriber, you can change your Presence status in myPortal for Desktop and myPortal for Outlook or via the menu controls of the voicemail box. Deactivating call forwarding at the telephone returns you to the **Office** presence status. For every change in the Presence status (except for **Office** and **CallMe**), you also define the scheduled time of your return to the **Office** or **CallMe** status.

As a subscriber, you can select the following statuses:

- **Office**
- **Meeting**
- **Sick**
- **Break**
- **Out of Office**
- **Holiday**
- **Lunch**
- **Home**
- **Do Not Disturb**

NOTICE: The system administrator can enable/disable the visibility of status "sick" within the system administration. See OpenScape Business UC Suite > Server

---

Call Forwarding to the Voicemail Box

If Presence status of a subscriber is not **Office** or **CallMe**, the communication system redirects calls for him or her to the voicemail box by default and notifies the callers via status-based announcements about the nature of absence and the scheduled time for return.

NOTICE: When a voicemail license is enabled, user's status is reset to **Office** and an active forwarding is cleared.

Info Text

You can enter any info text for your current presence status, e.g., "I am in Room No. ..." when attending a meeting. The info text is displayed in the Favorites list, in the internal directory and in the virtual conference room. The info text is deleted when you change your presence status.

Automatic Reset of the Presence Status

As a subscriber, you can have your Presence status automatically reset to **Office** at the end of your scheduled absence. Otherwise, the system extends the current Presence status in increments of 15 minutes until you change it yourself.

Visibility of your Presence Status

As a subscriber, you can specify for each subscriber in the internal directory whether or not that subscriber can see your Presence status other than **Office** and **CallMe** as well as the scheduled time of your return and any info text you may have entered.

NOTICE: Visibility settings are not applied for myAttendant users, as they can always see the presence status of other users.

Automatic Update of Presence Status via Outlook / iCal Appointments

As a subscriber, you can automatically control your Presence status via appointments (but not for those that have been proposed or declined) by using the specific keywords in the Subject line. You can choose between the following calendars:

- Exchange calendar (on the Microsoft Exchange Server)

  The automatic update of the presence status via Outlook appointments occurs independently, regardless of whether or not your PC is running. The administrator must configure the Exchange Calendar Integration for this function.

  NOTICE: Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Outlook calendar

  The automatic update of the presence status via Outlook appointments requires myPortal for Desktop or myPortal for Outlook to have been started on your PC.
- iCal calendar (myPortal for Desktop)

You can use the following keywords:

- **Meeting**
- **Sick**
- **Break**
- **Out of Office**
- **Holiday**
- **Lunch**
- **Home**

The keywords depend on the language set for the user interface. The keywords may be located anywhere in the Subject line. If the Subject line contains more than one such keyword, only the fist takes effect. When this function is enabled, your Presence status changes automatically at the start and end time of the relevant appointment. The check for calendar appointments occurs at 30-second intervals.

NOTICE: When enabling this function, please bear in mind that any appointments with corresponding keywords in the Subject line could lead to undesirable changes in your Presence

status. Consequently, you may nee to change the Subject line if needed.

NOTICE: The "sick" presence status may not be available, depending on system settings by the administrator.

Automatic Creation of Outlook Appointments when Absent)

As a subscriber, you can have appropriate Outlook appointments created automatically when you are absent by a change in your Presence status. The Subject line of the corresponding Outlook appointment consists of your Presence status and the text "(Auto)", for example: "Meeting (Auto)". The start and end times for the appointment involved correspond to your entries in myPortal for Desktop or myPortal for Outlook. The end time of the Outlook appointment remains unchanged in the event of a possibly delayed return. You can define whether the Outlook appointments should be stored in the local PST file or on the Exchange server. If you are using a local PST file, your Outlook must be open when creating the Outlook appointments. If you are using a PST file on the Exchange server, the Outlook appointments are created, regardless of whether or not your Outlook is open. The administrator must configure the Exchange Calendar Integration for this function.

NOTICE: Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

Screen Pops on Changing the Presence Status

As a subscriber, you can have changes to your Presence status indicated by a screen pop.

13.4.2 CallMe Service

The CallMe service enables subscribers to define any phone at an alternative workplace as the CallMe destination at which they can be reached through their own internal phone numbers. The subscriber can use myPortal for Desktop or myPortal for Outlook at his or her alternative workplace exactly as in the office and thus also make outgoing calls from the CallMe destination.

Inbound Calls

Inbound calls to the internal phone number are forwarded to the CallMe destination. The internal phone number of the called subscriber is displayed to the caller. Unanswered calls are forwarded to the voicemail box after 60 seconds.

NOTICE: If an unconditional forwarding for the controlled device is configured, Application Launcher cannot receive call related events from the communication server and cannot therefore trigger any actions toward applications. This also applies when the UC Suite feature CallMe is activated.

Outbound Calls

For outbound calls with myPortal for Desktop or myPortal for Outlook, the communication system sets up two connections. It first calls the subscriber at the CallMe destination. If the call is answered, the communication system then calls the desired destination and connects the subscriber with it. The internal phone number of the caller is displayed at the destination (One Number Service).

Presence Status

When the CallMe service is enabled, the message "`CallMe active`" appears in the display of the relevant phone (not for analog and DECT phones). Other subscribers see the presence status **Office**.

Activation

As a subscriber, you can activate the CallMe service manually. In addition, the Call-Me service is also reActivated by an automatic reset of the Presence status following an absence, provided it was active earlier. Then following types of CallMe destinations are not supported:

- Group
- Redirected telephone

Displaying the CallMe Destination in the Favorites List

As a subscriber, you can have the number of your CallMe destination displayed in the Favorites list of other subscribers instead of your own phone number.

Deactivation

The CallMe service remains active until your Presence status changes.

NOTICE: CallMe function should not be used when dialing or caling in an open conference.

13.4.3 Status-based Call Forwarding

Status-based call forwarding enables subscribers to forward calls based on their Presence status to one of their additional phone numbers or their voicemail box.

As a subscriber, you can configure status-based call forwarding for every presence status except **Office**, **CallMe** and **Do Not Disturb**. When you change your Presence status, the communication system activates call forwarding to the destination defined by you for this purpose. For example, if you are away from the office, to your mobile phone or if you are on vacation, to your representative.

13.4.4 Rule-Based Call Forwarding

Rules-based call forwarding enables subscribers to forward calls based on numerous conditions and exceptions even more flexibly than with status-based call forwarding.

In addition, rule-based call forwarding also supports:

- Any destinations
- Presence status **Office**, **Meeting, Sick, Break, Out Of Office, Vacation, Lunch, Home**

NOTICE: CallMe and **DND** are not valid for rule-based call forwarding.

As a subscriber, you can define rules and activate or deactivate them at any time by using the Rules wizard. A rule can only be active if your phone has not been forwarded. Status-based call forwarding (except to the voicemail box) overrides rule-based call forwarding.

When a call forwarding rule is active, **"rule active"** appears on the display of your telephone.

When an inbound call is received, the communication system checks the applicability of the active rule in accordance with its sequential order in the Rules wizard. Only the first applicable rule is executed. In this case, your phone will ring once, and the communication system will then forward your call to the defined destination.

You can define several types of conditions and exceptions (except when ...) in one rule. However, you cannot define a condition with an exception of the same type. For example, it is not possible to define a condition of the type "On certain weekdays" together with an exception of the type "Except on certain weekdays".

Types of Conditions and Exceptions

- (except) for certain Presence status
- (except) from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) when transferred to you from certain people (in the internal directory, external directory, personal directory or from any station number)
- (except) from a certain type, i.e., **internal**, **external** or **Unknown Contact**
- (except) on a certain date (also on multiple dates)
- (except) on certain weekdays
- (except) between a certain Start and End date
- (except) between a certain Start and End time

13.5 Directories and Journal

Directories, the Favorites List and the Journal organize contacts and calls.

13.5.1 Directories

Directories are used to organize the contacts of subscribers. Subscribers can access these contacts with UC Suite clients and via system phones with displays.

The system provides the following directories, which support the following functions and with the below priority for lookup number (lookup number will be

supported only for external call and in case that CO/ITSP does not provide the name):

Directory	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	System telephone with a display
Outlook Contacts MAC OS contacts (myPortal for Desktop)	If required, the subscriber can import Outlook/Mac OS contacts on starting myPortal for Desktop when using Microsoft Windows.	Contains the personal Outlook contacts of a subscriber. Only the subscriber involved has write access to this data.	Contains the personal Outlook contacts of a subscriber. Only the subscriber involved has write access to this data.
Personal directory	The subscriber can either import Outlook/Mac OS contacts on starting myPortal for Desktop or maintain personal contacts manually. Imported contacts cannot be edited.	-	Outlook contacts imported via the Personal Assistant.
Internal directory	The internal directory of UC Smart offers additional features with the UC Suite. It contains: • All internal subscribers • Groups for which the display has been activated in the system • Additional phone numbers, if the subscriber has made this information visible to other internal subscribers Internal subscribers (with system telephones) are displayed with their Presence status and can be contacted through Instant Messaging. The Presence status of a subscriber can only be shown if allowed by that subscriber. If relevant, the scheduled time of return and any info text that may have been entered by the subscriber are also displayed. A subscriber has only read-access to this directory. Internal directory includes the System directory. But searches done in the Internal directory do not include System directory results, but only Internal directory entries.		Contains all internal subscribers and groups for which the display has been activated in the system.
External directory	Contains contacts from a corporate directory and must be configured by the administrator. A subscriber is only provided read-access to this directory.		-
Public Exchange folder (not usable with Office 365)	Contains contacts of the public Exchange folder if configured by the administrator. These are shown in the external directory. Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
External Offline Directory (LDAP)	Contains contacts from the LDAP corporate directory and must be configured by the administrator. The external offline directory can only used for searches. The administrator can enable and disable the display of the external offline directory for system telephones.		

Directory	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	System telephone with a display
System Directory	Contains all system numbers, UC and non UC users. Non UC users include stations with no UC licenses and virtual stations, like Fax, AutoAttendant. System Directory does not apply to the Fax Printer		Includes all internal stations and all central speed-dial numbers. The administrator can enable and disable the display of a subscriber in the system directory.

NOTICE: Phone numbers stored in user settings and all directories (internal, external, personal, outlook, exchange) should be in canonical format in order to be reachable both from UC and device.

Access code should not be in the number.

NOTICE: When adding or removing a UC contact, it may take several minutes (**and** up to 30') until changes are applied on all clients and devices due to caching mechanisms that are used. Alternatively a system restart can be performed for the changes to take **immediate** effect.

Simple Search

As a subscriber, you can search the directories by **First Name**, **Last Name** or a call number. The directories are searched in the order shown in the table above. The search can be conducted using whole words and also with partial search terms such as a part of a station number, for example. The set search options remain in effect for subsequent searches. Al search terms used are saved. You can optionally delete the list of search terms used.

Advanced Search

You can selectively search in the **Title**, **First Name**, **Last Name**, **Company**, **Extension**, **Company Ph.**, **Business Ph. 1**, **Business Ph. 2**, **Home Ph. 1**, **Home Ph. 2**, **Mobile Number** and **Email** fields and limit the maximum number of hits. The modern interface of myPortal for Desktop does not support the advanced search. In a device only **Business Ph. 1**, **Home Ph. 1**, **Mobile Number are supported.**

Sorting

The contacts of a myPortal for Desktop and myPortal for Outlook directory can be sorted by any column in ascending or descending alphanumeric order. The modern interface of myPortal for Desktop does not support sorting.

13.5.1.1 How to Configure Directories for System Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile.

You can select which directories are to be made available on system telephones with displays.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **Display**.
4) Select one of the following options in the **Directory (phone book)** drop-down list:
   - If all the personal contacts, the internal, external and networking directory and the LDAP directory are to be made available, select **All**.
   - If only the personal contacts, the internal, external and networking directory is to be made available, select **Internal**.
   - If only the LDAP directory is to be made available, select **LDAP**.
   - If no directory is to be made available, select **No**.

   NOTICE: The user can activated the search/lookup requests to be handled as requests to the Unified directory, by selecting the **Internal Phonebook via Unified Directory**. 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) Click **Apply**.

Next steps

If you have selected **All** or **LDAP**, make sure that an appropriate LDAP directory (e.g., Open Directory Service) is available for the system telephones.

13.5.2 Internal Directory

The internal directory contains the contact details of the internal subscribers of the communication system. UC Suite clients can access the system directory.

As an administrator, you have unrestricted access to all data in the internal directory. As a subscriber, you can dial from the internal directory.

The administrator can disable the display for all analog stations or for analog stations without an associated name. Subscribers whose names begin with - are not displayed in the latter case.

13.5.2.1 How to Enable or Disable the Display of Analog Stations in the Internal Directory

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

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) In the **Analog Extensions** area, select one of the following options from the **Analog User Mode** drop-down list.
   - If all the analog stations are to be displayed in the internal directory, select **Show all**.
   - If only analog stations with a name are to be displayed in the internal directory, select **Show named only**.

     NOTICE: Analog stations with names beginning with '**-**' are not displayed in the latter case.

   - If no analog stations are to be displayed in the internal directory, select **Not shown**.
6) Click **Save**.

13.5.2.2 How to Enable or Disable Searching the Internal Directory only

When dialing by name, you can configure either limiting the search only in the internal directory, or searching all directories in the network environment. The system is configured by default to search only in the internal directory.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

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.

   NOTICE: The check box **Dial by name search local extension only** is enabled by default.

   The system now searches only the internal directory when dialing by name. When the local extension is reached, the system plays the receiver's name, as long as it has been previously recorded.
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.

   The system now searches all directories in the network environment when dialing by name.

13.5.3 External Directory

The external directory includes contacts from outside the communication system.

The data of the external directory is available to all subscribers in all UC Suite clients and the phone display. Subscribers can dial from the external directory. Users with the UC Suite clients myAttendant and myAgent can also edit data in the external directory.

Importing a CSV File

As an administrator, you can import contacts from a CSV file in UTF-8 encoding from the local file system or a network share into the external directory.

A header in the CSV file allows the mapping of field names in the CSV file to fields in the system. A typical CSV file may be structured as follows:

- Header line:

  "Customer ID","Last Name","First Name","Company Phone Number","Company Name":
- Data line:

  "987654","Dubios","Natalie","+498977712345","Company"

You can map the data being imported from the CSV file to the following fields in the system:

- Customer ID
- Title
- First Name
- Last Name
- Company
- Business Ph.
- Business Ph2
- Mobile Ph.
- Home
- Fax Ph.
- E-mail
- City

NOTICE: The contact name will be displayed in the call history, only if you fill in both the First Name and Last Name fields.

After processing the CSV template, the file must be in saved in UTF-8 format in order to ensure the correct import of any existing special characters.

If you want the import to overwrite data, the corresponding **Customer IDs** should be identical.

NOTICE: A CSV template and a description of the syntax required for importing data into the external directory can be found under **Service Center** > **Documents** > **CSV Templates**.

13.5.3.1 How to Import a CSV File from the Local File System into the External Directory

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

A suitable CSV file in UTF-encoding with data for the external directory is available in the local file system.

There are certain limitations to the length of the fields in the CSV templates. These length limitations are listed below:

- customer_business character varying(50)
- customer_business2 character varying(50)
- customer_home character varying(50)
- customer_mobile character varying(50)
- customer_title character varying(20)
- customer_firstname character varying(50)
- customer_surname character varying(50)
- customer_company character varying(255)
- customer_id character varying(255)
- customer_xmppid character varying(256)
- customer_fax character varying(50)
- customer_email character varying(255)
- customer_city character varying(255)
- customer_street_address character varying(2048)
- customer_import_source character varying(256)

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click **Edit** to start the **External Directory** wizard.

4) Click on **Import External Directory** tab.

5) Select one of the following options:

- If you want to load the CSV file from the local file system, select the **Local file** radio button and navigate to the CSV file in the **File Upload** area.
- If you want to load the CSV file from a network share, select the **Public Windows Folder** radio button and enter the network share access data (name of the CSV file, domain name as well as user name and password for the share) in the **Public Windows Folder** area.

  Verify your input by clicking on **Test**.

6) Click in the **File Upload** area on **Choose File** and select the desired file.

7) Enter the number of header rows in the CSV file in the **Header Rows** field.

8) Enter the **Field separator** used in the CSV file.

9) Select one of the following options:
   - If you want to delete the existing data from the external directory, select the check box **Remove data before import**.
   - If you do not want to delete the existing data from the external directory, clear the check box **Remove data before import**.

   NOTICE: The flag **Remove data before import** will not remove records if they are already used in other functions such as a VIP caller, etc.

   NOTICE: The **Remove data before import** flag only deletes data which is imported from CSV import. Manually imported data is not deleted to avoid unexpected data loss. The only way to delete manually entered data is to delete them manually.

10) In the **Duplicate Customer ID** area, select how the system should respond when trying to import data with existing customer IDs:
   - If you want the existing contacts to be overwritten by the data from the CSV file, select **Update existing customer**.

     NOTICE: CustomerID is the identifier that determines whether two records are duplicates. Thus, it is considered that imported records with an existing CustomerID refer to an existing customer and they will be updated. The **Update existing customer** flag only works when CustomerID is mapped during import. It is strongly advised that you rely on the provided template and adapt the data over it, without omitting unique identifiers.
   - If you want to keep the existing contacts, select **Stop importing current record**.

11) Click **Next**.
12) Select the fields of the CSV file to be mapped to corresponding fields in the system sequentially from the drop-down lists. If the appropriate fields do not exist or if you do not want to import the data, click on the blank option.
13) Click **Next**.
14) Click **Import**. Do not close this window while the data is still being imported. On completing the import, the number of imported records is displayed.

13.5.3.2 How to Add Access to an External Database for the External Directory

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The required data for accessing the external database is available.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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 How to Export a CSV file from the External Directory

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on the **Export External Directory** tab.
4) Select one of the following options:
   - If you want to export a CSV file in the local file system, select the **Local file** radio button and click on the **Start** button.
   - If you want to export in a public Windows folder, select the **Public Windows Folder** radio button. Enter the requested values in the following fields:

     - **Filename**

     - **Username**

     - **Domain**

     - **Password**

     And click on the **Start** button.

13.5.4 External Offline Directory (LDAP)

The external offline directory (LDAP) contains contacts from an LDAP server for myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook and for system telephones with displays.

The system supports LDAP Version 2 with authentication.

LDAP (Lightweight Directory Access Protocol) is a TCP/IP-based directory access protocol for accessing network directory services. LDAP has a unique format world-wide in which all names can be represented. It provides for different layouts and enables unique associations between names and their internal representation. This data is defined by the administrator together with the IT administrator of the customer when planning and setting up a project. LDAP can be used under the MS Windows and Linux operating systems.

In a Microsoft environment, the Active Directory Server (ADS) or the Exchange Server also serves as the LDAP server. Under Microsoft Windows, user data can be administered with the Active Directory (AD) application or ESTOS

Metadir, for example. The administration of this data is generally performed by the IT administrator of the customer.

Under Linux, the user data can be administered with OpenLDAP, for example.

Setting up an LDAP directory service can be simplified with an LDAP browser (e.g., the freeware from Softerra).

Phone numbers on the LDAP server may only include "-" and blanks as delimiters. Other delimiters cannot be filtered out by the system.

As an administrator, you can adapt the mapping of fields to the names of the used LDAP server during the configuration of an external offline directory. Deleted fields are ignored when searching for names via phone numbers. The search always occurs with the last 4 positions of the phone number preceded by a wildcard. You can deactivate the search for names via phone numbers for incoming calls.

If the default port 389 is already being used, some other port must be configured

---

NOTICE: More information can be found on the Internet at `http://wiki.unify.com`.

The data of the external directory is available to subscribers in myPortal for Desktop, myAttendant, Fax Printer and myPortal for Outlook during the search.

System Telephones with Displays

As a subscriber, you can select between the internal directory and the LDAP directory via the menu., provided these have been configured for system telephones. The LDAP directory supports searches in the appropriate contacts and the subsequent calling of a contact.

The name information provided by the LDAP server is not displayed in ringing or call status. The call numbers for incoming calls are also not replaced by the name information provided by the LDAP server (as when call numbers are replaced by SSD names).

A system subscriber can only be reached from the LDAP directory if a DID number was configured for him or her and if this entry corresponds to the entry in the LDAP database. Call numbers provided by the LDAP server can only be routed within the network if the internal call number and the DID number are identical.

13.5.4.1 How to Add the External Offline Directory (LDAP) for PC Clients

Prerequisites

You are logged into the WBM with the **Expert** profile.

You know the required access data for LDAP server.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.

3) Click the **External Providers Config** tab.
4) Select one of the following options:
   - If you want to enable the resolution of phone numbers into names in the journal for external incoming calls, select the **Search by phone number** check box.
   - If you want to disable the resolution of phone numbers into names in the journal for external incoming calls, clear the **Search by phone number** check box.
5) Click **Add**.
6) Enter the access data of the LDAP server.
   a) Enter a name for this external offline directory under **Name**.
   b) Enter the name or the IP address of the LDAP server under **Server**.
   c) Enter the port number of the LDAP server under **Port**.
   d) Under **LDAP Basic DN**, enter the LDAP Base Distinguished Name, e.g., `dc=example-for-a-domain, dc=net`.
   e) Enter the **User Name**.
   f) Enter the **Password**.
7) Enter the corresponding field designation of the LDAP server for the following fields: **Title**, **First Name**, **Last Name**, **Business Ph. 1**, **Business Ph. 2**, **Home**, **Mobile**, **Company**, **Company Ph.**, **Postal Address**, **State, province or county**, **Country**, **Postal Code**, **E-mail**, **Pager**, **Fax Number** and **City**.
8) Click **Save**.

13.5.4.2 How to Delete the External Offline Directory (LDAP) for PC Clients

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click the **External Providers Config** tab.
4) Click on the external offline directory to be deleted.
5) Click **Remove**.

13.5.4.3 How to Add an External Offline Directory (LDAP) for System Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile.

You know the required access data for LDAP server.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.

3) In the menu tree, click on **System** > **LDAP**.
4) Enter the **IP address of the LDAP server**.
5) Enter the **Port number for LDAP access**.
6) Enter the **User Name**.
7) Enter the **Password**.
8) Enter the password again in the **Confirm password** field.
9) Under **Basic DN**, enter the LDAP Base Distinguished Name of the LDAP server, e.g., `dc=example-for-a-domain, dc=net`.
10) Under **Search query**, enter the search string for the LDAP server, e.g.: `cn=$*`.
11) Enter the **Result attribute, Name** for the LDAP server, e.g.: `cn`.
12) Enter the **Result attribute, Station number** for the LDAP server, e.g.: `telephoneNumber`.
13) Select one of the following options for sorting the search results:
    - If you want to have the search results sorted, select the **Sort search results** check box.
    - If you do not want to have the search results sorted, clear the **Sort search results** check box.
14) Enter the **LDAP seizure code**.
15) Enter the **LDAP station number prefix**.
16) Click on **Apply**.

13.5.5 System Directory

Regarding UC Suite clients, the system directory contains all system numbers, UC and non UC users. Non UC users include stations with no UC licenses and virtual stations, like Fax, AutoAttendant. Regarding devices, the system directory contains all internal stations and all central speed-dial numbers.

The administrator individually disable the display for every subscriber and every speed-dial number with a name.

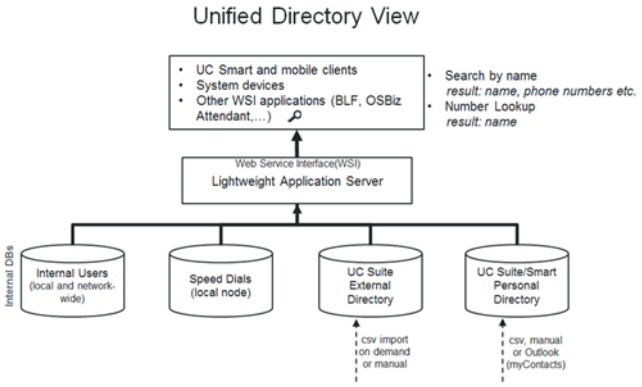
13.5.6 Unified Directory

OpenScape Business provides different data sources to store and to retrieve user or contact related data, starting with the internal user data in the internal user configuration, via the internal speed dial list, up to the different directories of the UC applications.

Each data source within OpenScape Business is used by a specific client application either located within the system SW itself in the phone devices or within a UC client application. Depending on the used data sources and the used clients, the retrieved data and their presentation is different.

The "Unified Directory" service within OpenScape Business comprises the existing OpenScape Business data sources for common search and name resolution functions. It provides the same search result or name resolution information to all system devices and OpenScape Business clients.

The Unified Directory service can either be accessed via the Web Service Interface (WSI) from externally located clients like myPortal to go or internally via the call processing mechanisms (e.g. from OpenStage Phones).



Unified Directory uses following internal databases and directories of OpenScape Business:

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

The Unified Directory service is available within every OpenScape Business system from V2R2 on. It does not require specific HW-SW or license prerequisites.

In order to get best results when using the Unified Directory some rules regarding phone number formats and writing of names have to be followed.

13.5.6.1 Features

Supported Devices / Clients

Unified Directory Service provides:

- Directory Search in several internal data sources of OpenScape Business
- Unified offering of the search result to all supported clients
- Phone number Look-Up / Name Resolution in several internal data sources
- Unified offering of name resolution results for all supported clients
- External data access via the WebServices Interface (WSI)

The features are available for single node systems as described in the following. Within OpenScape Business networks, the availability of the features depends mainly on the kind of connection of the trunks, devices and clients within the network.

Unified Directory supports following clients / system devices of Unify using the indicated interfaces:

Device/Client	Used Interface/ Protocol	Remarks
OpenStage phones	Call Processing / CorNet protocol	WSI / HTTP(S) is optional on OpenStage 60/80 for caller images
OpenScape Deskphone IP	Call Processing / CorNet protocol	WSI / HTTP(S) is optional on DeskPhone IP 55 for caller images
Cordless (CMI) devices	Call Processing / CMI protocol	
CP 100/110 /200/205/210/ 405	Call Processing / CorNet protocol	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI / HTTP(S)	
myPortal @work	WSI / HTTP(S)	
myPortal to go	WSI / HTTPS	
Openscape Business Attendant/BLF	Call Processing / CorNet protocol	WSI / HTTP(S) is optional

NOTICE: The UC Suite myPortal, myAttendant and myAgent clients use their own mechanisms for directory search and name resolution.

Search function

The Unified Directory search is always performed by using the specific device / client user interface. The search criteria and the used character set could be restricted, depending on the used clients.

After the search criterion is entered the search is performed within subsequent directories

- Internal user directory (network wide)
- Speed dial lists
- UC Smart Personal Directory (optional)
- UC Suite External Directory (optional)
- Personal Outlook Contacts (if imported via myContacts)

All matches within the directories above are shown as search results together with their origin. The matches contain either the full contact data set or only parts of it. The information depth of the results depends on the data source.

NOTICE: Group name search in myportal@work is not supported at UC Suite mode. Only licensed users (basic license) and licensed MULAP groups (UC Entries) search is supported.

The matches are presented at the devices or clients depending on display capabilities.

	Internal User Directory	Speed Dials	UC Smart Personal Directory	UC Suite External Directory	Personal Outlook Contacts (via my Contacts)
Last Name	X	---	X	X	X
First Name	X	---	X	X	X
Short/ Displayname	X	X	---	---	---
Office Phone No.	---	---	X	X	X
Home/Ext. PhoneNo.	---	---	X	---	X
Mobile Phone No.	---	---	X	X	X
Email-Adr.	---	---	X	X	X
Company name	---	---	X	X	X
City	---	---	---	---	---
Contact Picture	---	---	X	---	X
Contact Picturepreview	---	---	X	---	X

Phone Number Look-Up

Unified Directory Phone number Look-Up resolves the transferred calling party (CLI) by a number search in all supported internal data sources . The search is perfomed within following phone number fields:

- Office number
- Mobile number
- Home number

The Phone number Look-Up is triggered in case of incoming or outgoing calls in general, whereas specific routing and forwarding features are considered in addition.

A fixed prioritization of the data sources that are used for Phone number Look-Up is implemented in order to get the result as fast as possible. The result contains either only lastname, firstname, displayname or ,if available, the full related contact data.

Table 7: Supported Data Sources and Prioritization

Priority	Data Sources	Remark
1	CO/ITSP name (as sent by provider)	Prerequisite is to enable flag "Name in CO".
2	Speed dial list	
3	Personal Contacts	

Priority	Data Sources	Remark
4	UC User detail	

The retrieved data are presented on the user's device and/or in the UC client. The information depth depends on the display capabilities.

- **Incoming calls**

  Supported scenario for single node systems:

  – Basic call
  – Group call/ MULAP call
  – Ringing Group
  – Single Step Call Transfer (SSCT)
  – Attended/Supervised/Consultation Transfer
  – Call Forwarding Unconditional (CFU)
  – Call Forwarding No Reply (CFNR)
  – Call Forwarding Busy (CFB)
  – Blind transfer
  – Call Pickup

  NOTICE: Call Pickup is different from Call Pickup Group. In Call Pickup Group, when an external number is saved to the Unified Directory, the name of the caller is not shown from the members of the group.

  Supported scenario for multi node (network) scenarios is a Gateway Call.
- **Outgoing call**

  In case of an Outgoing Call the Phone number Look-Up of the called party number happens only once.

  Supported scenario for single node systems is a Basic Call to external number.

The presentation of the Phone number Look-Up result depends on display capabilities of the phones.

13.5.6.2 Rules and Conventions

Some conventions regarding number and name formats within the data sources have to be observed in order to get optimal results using the Unified Directory service.

Supported Number Format

All external phone numbers within the data sources must be entered in the canonical format including country and area code. e.g.+4989700712345

Speed Dial list supports only system dialable format e.g. 0089700712345 or 0004989700712345

When Speed Dial numbers are configured to be accessible through LDAP, you have to enable the Number conversion option to display the contact name when the number is in canonical format. For more information on how to enable

Number conversion, see How to Add an External Data Source for the Open Directory Service on page 1127.

Supported Name Formats

The following conventions regarding name formats and character sets have to be observed:

- **Speed dial name format**

  Name search within the Speed Dial List is supported only with specific configuration rules. The first and last names have to be entered within the existing name field using the following pattern:

  <Last Name>, <First Name> (comma separated)
- **Internal Users in case of Migrations**

  Migration to V2R1 and onwards with internal users that do not follow these configuration rules will not be supported in the expected way. This means the administrator should convert internal names to the following pattern before migration:

  <Last Name>, <First Name> (comma separated)

Availability of directory changes

After creating, updating or deleting contacts in the various data sources it can take up to 10 minutes until all changes appear on Phone number Look-Up results.

13.5.6.3 Functional Boundaries

The following functional boundaries do exist regarding Unified Direcrories:

Name Search

- Group name support

  Group names (not MULAP names) can not be searched in all kind of configurations
- Support of special characters

  On most phone devices the user can search for standard characters "a-z". Special (diacritical) characters like German characters Ää,Öö,Üü, ß are not accessible via phone device user interface.

  Therefore a plain character search result includes also special characters. A search for any of the characters "acdegilnorstuyz" matches with the corresponding special characters "àáâãäåąăçćčďđèéêëęěğìíîïĺľłñńňòóôõöőřŕšśşťùúûůüűýÿžżź"

  in the search result.

  NOTICE: Phonebook search with the wildcard character at the beginning of the search string, e.g. <*jo*>, is only supported for internal users.

- Support of Speed Dial Name format

  Name search within the Speed Dial List is supported only with specific configuration rules. The first- and last names have to be entered within the existing name field using one of the following patterns

  – <Last Name>, <First Name> (comma separated)
  – <First Name> <Last Name> (space separator on this case)

Name Presentation

Personal Contacts in UC Smart and from external offline directory, with length of first name plus length of last name greater than 24 characters, will be truncated to 24 characters length to fit the display length of the devices.

Phone number Look-up

The Phone number Look-Up feature (retrieve contact name from calling party number) is not supported in Unified Directory for SIP and S0 devices.

13.5.6.4 Unified Directory in Networked Systems

The Unified Directory Service is active within every node of an OpenScape Business Network and uses the datasources of the own system. Phone Devices and Client use always the Unified Directory Service within their own node.

Therefore it depends on the kind of datasource content if netwide contacts are available.

Table 8: Local and Netwide Datasource

Data source	Local data	Netwide data
Internal user directory	X	X
Speed dial lists	X	---
UC Smart Personal Directory	X	---
Personal Outlook Contacts (via myContacts)	X	---

NOTICE: The unified directory is not fully supported in mixed UC Suite/ UC Smart environments.

Phone number Look-up

In Networking scenarios the Phone number Look-Up functionality is not used. In such scenarios the name is transported via normal networking mechanisms between the network nodes.

For internal users the configured Display Name is used so Lookup is not required.

13.5.6.5 How to Import Contacts to Unified Directory

Import contacts wizard offers the functionality to import directory contacts from a csv file.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Unified Directory**.
3) Click on **Edit** next to **Import Contacts**, to proceed with the importing of the contacts to the Global Directory.
4) Under **File Upload** section, click on **Choose File** and select the desired csv file to upload.

   NOTICE: The maximum amount of entries per import is 100,000 (30,000 for embedded systems).

5) Under **Options** section, enter the **File separator**. ';' or ',' are valid entries.
6) Click **OK & Next**.
7) Backend processes the file, reads the headers and presents the headers together with the predefined categories of the Master Directory into the **CSV Header Mapping** page. Then the user can match the entries of the csv files in order to import the relative data to desired categories other than the predefined.
8) Click **OK & Next**.
9) Into the **Overview of Import** page:
   a) Select one of the following options about the imported csv file:
      - Append global directory contacts
      - Delete all global directory contacts imported via CSV
      - Delete all global directory contacts
   b) Regarding **Duplicated Customer ID** select one of the following options:
      - Update existing customer
      - Stop importing current record

   The entries which will be added and the entries which failed to be validated are presented into two corresponding tables.

   NOTICE: Duplicate records are identified by combination of First Name, Last Name, Business Phone and Email fields. These fields cannot be automatically updated by

choosing "**Update existing customer**". In order to update these fields, choose to delete first older records in step 9a.

The flag **"Update existing customer"** only works when Customer ID is mapped during import.

Only record with the same **Customer ID** will be considered as "existing customer" and will be updated.

Flag "**Remove data before import**" will not remove records if they are already used in other functions such as used as a VIP caller, etc.

Customer ID is the only key to determine if the record is duplicated. If Customer ID is not mapped, there is no way to avoid duplicates.

Therefore, it is strongly advised that customers rely on the provided template and adapt their data over it without omitting unique identifiers.

---

10) Click **OK & Next**. Several minutes may be required for this process.
11) **Import Finished** page informs regarding the number of the entries which were imported.
12) Click on **Finish**.

13.5.6.6 How to Edit or Add new Unified Directory Contacts

Edit contacts wizard offers the functionality to edit the already imported contacts or add a new one.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Unified Directory**.
3) Click on **Edit** next to **Edit Contacts**, to proceed with the editing of the contacts of the Global Directory.
4) Edit the desired fields of the contacts. Only when an entry is edited then **Apply** button becomes available.
5) Click on **Add** to manually add a new contact.
6) Fill the desired fields of the new contact and click on the **Apply** button.

13.5.7 Departments

Departments classify subscribers in the internal directory into groups based on their organizational affiliation. The internal directory allows you to search and sort by department.

13.5.7.1 How to Add a Department

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Departments** wizard.
4) Click on **Add**.
5) Enter the **Department Name** of the Department.
6) Enter the **Hunt Group** identifier.
7) Click on **Save**.

13.5.7.2 How to Assign Stations to a Department

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard.
4) Select the relevant station.
5) Click on **Edit** > **Personal Details** > **My Personal Details**.
6) Select the desired department from the list box in the **Department** field.
7) Then click **Save**.

13.5.7.3 How to Edit a Department

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Departments** wizard.
4) Click in the list of departments on the appropriate department.
5) Click on **Edit**.
6) Enter the **Department Name** of the Department.
7) Enter the **Hunt Group** identifier.
8) Click on **Save**.

13.5.7.4 How to Remove a Department

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Departments** wizard.
4) Click in the list of departments on the appropriate department.
5) Click on **Remove**.
6) Click on **OK**.

13.5.8 Favorites List

The Favorites list provides you (as a subscriber) with a constant view of selected contacts. These contacts can also be called very easily directly from the Favorites list. All internal subscribers with system telephones and external communication partners are shown together with their Presence status and can be contacted via instant messaging.

As a subscriber, you can add contacts from all directories to the Favorites list. For favorites that do not come from the internal directory, instead of the symbol for the Presence status, the symbol for the source of the contact is displayed.

The Favorites list manages contacts in groups. The contacts in all groups can be sorted by First Name, Last Name or their original sorting order.

When an internal subscriber is absent, you can determine the scheduled time of his or her return by positioning the mouse pointer over the entry for that subscriber, provided the subscriber has allowed his or her Presence status to be visible to you.

For favorites with multiple phone numbers, you can specify a default number with which the contact is to be called. The default phone number of a favorite can be determined in the context menu from the symbol with the activated check box.

13.5.9 Journal

The journal is the list of all incoming and outgoing calls of a subscriber. It enables subscribers to quickly and easily respond to missed calls and call back their contacts or call them again directly from within the journal.

Folder for Call Types

The calls are arranged in the following groups:

- **Open**

  Contains the unanswered missed calls for which a call number was transmitted. As soon as one of these calls is answered, all associated entries with that call number are dropped from the list.

- **All calls**
- **Missed**
- **Answered**
- **Internal**
- **External**
- **Inbound**
- **Outbound**
- **Scheduled**

  Contains all the calls that you (as a subscriber) have scheduled for specific dates/times. The Scheduled Calls feature is not available to Contact Center agents. In order for the communication system to execute a scheduled call, myPortal for Desktop or myPortal for Outlook must be open at the scheduled time; your presence status must be **Office** or **CallMe**, and you must confirm the execution of the call in a dialog. If you are busy at the time the scheduled call is to be made, the system defers the scheduled call until you are free again. myPortal for Desktop or myPortal for Outlook informs you of any pending scheduled calls on exiting the program. On starting the application, myPortal for Desktop or myPortal for Outlook notifies you about any scheduled calls for which the scheduled time has elapsed. You can then either delete such calls or save them with a new scheduled time.

Not all folders for call types are available in the modern user interface myPortal for Desktop.

On starting the modern user interface myPortal for Desktop, only 100 journal entries are loaded. After that and when new calls come in, the number in call history will exceed 100 records.

Retention Period

The system saves a record of the calls in the Journal for a maximum period of time, which can be configured by the administrator. As a subscriber, you can reduce this time. After the retention period expires, the system automatically deletes all associated entries.

NOTICE: The retention period also determines the maximum time period for evaluations with myReports.

Grouped by time period

The calls in each group are arranged by time, e.g.: Today, Yesterday, etc., Last Week, Last Month and Older. Your administrator can set the duration for which calls should be saved in the Journal. After this set time period expires, the entries are automatically deleted. The grouping by time period is not available in the modern user interface of myPortal for Desktop.

Call Details

Every call is shown with the Date and Time and, if available, with the call number. If a directory contains further details on the call number such as the **Last Name**, **First Name** and **Company**, then this information is also shown. In addition, the **Direction**, **Duration** and **Call Complete** columns are also displayed in most folders. Not all call details are available in the modern user interface of myPortal for desktop.

Sorting

You can sort the calls in the Journal by any column in ascending or descending alphanumeric order.

You can jump within the Journal to the first call whose entry begins with a specific character in the sorted column, e.g., to the first Last Name beginning with "P". By entering subsequent characters, you can then narrow the search. Sorting is not available in the modern user interface of myPortal for Desktop.

Export

As a subscriber, you can export the journal as a CSV file using myPortal for Desktop or myPortal for Outlook:

13.5.9.1 How to Change the Maximum Retention Period for the Journal

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **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.

   NOTICE: The retention period also determines the maximum time period for evaluations with myReports.

6) Click on **Save**.

13.6 Calls

For calls, convenient features such as a desktop dialer, screen pops and the option to record calls and conferences are available to subscribers.

13.6.1 Desktop Dialer and Clipboard Dialer

The Desktop Dialer and Clipboard Dialer enable users with myPortal for Desktop (Windows) or myPortal for Outlook to call a selected destination or a destination copied to the Windows clipboard via a key combination from many Windows applications, e.g., from an Outlook e-mail.

Depending on the type of string used, the Dialer works as follows:

- A phone number in canonical format is dialed directly.

- A station number in dialable format is dialed directly if the communication system can decide whether an internal or external destination is involved. Otherwise, the user is asked to make the appropriate selection.
- A string containing letters is searched in the directories as a first name or company.

The Desktop Dialer and Clipboard Dialer are executed after a definable time period. During this period, the dialing can still be canceled. If the preset value of 3s is changed to 0s, the dialing will be executed immediately. The value is changed in the settings of the UC Suite clients.

Windows applications that were implemented with standard Windows-compliant components usually support the Desktop Dialer and Clipboard Dialer, but 16-bit applications do not. The Desktop Dialer is only supported by 32-bit applications.

13.6.2 Screen Pops

Screen pops in the UC Suite clients offer you convenient ways to respond to incoming calls or new voicemails with a single mouse click, for example.

Screen pops appear in the lower right corner of the screen. There are different types of screen pops. Screen pops for calls and messages show phone number, name and image of the caller, if possible. The buttons in the screen pops change, depending on the situation.

Screen pops can be minimized to a tray icon. As soon as more than three screen pops are opened for calls, they are automatically minimized and shown as icons on the task bar.

13.6.3 Record calls

A subscriber can record calls. Recorded calls appear in the voicemail box.

INFO: Note that in most countries you are legally required to notify the other party that you are recording the call. In some countries (such as France, for example), the other party is automatically notified by the system.

As an administrator, you can allow or prevent the recording of calls and conferences on a system-wide basis. In addition, you can optionally configure the playback of an announcement or warning tone at the start of the recording.

As a subscriber, you can control the recording of calls via myPortal for Desktop or myPortal for Outlook. Recorded calls are identified in the voicemail box with a red dot and show the call number of the other party if available.

Ongoing recordings are automatically stopped by a consultation hold, placing a call on hold, transfers and the initiation of a conference.

NOTICE: DTMF is not supported during call recording.

13.6.3.1 How to Activate or Deactivate the Recording of Calls

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Live Record**.
5) Select one of the following options:
   - 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) Click on **Save**.

NOTICE: Calls that have this functionality activated cannot be transferred or held.

13.6.3.2 How to Activate or Deactivate the Recording Announcement

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Live Record**.
5) Select one of the following options:
   - 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) Click on **Save**.

13.6.3.3 How to Activate or Deactivate the Warning Tone for Recording

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Live Record**.
5) Select one of the following options:
   - If you want to play a warning tone at the start of a recording, select the **Play pip tone before recording** check box.
   - If you do not want to play a warning tone at the start of a recording, clear the **Play pip tone before recording** check box.
6) Click on **Save**.

NOTICE: 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 Conferences

In a conference, multiple participants (including external parties) can communicate with one another at the same time.

13.7.1 Conference Management

Conference management enables subscribers to use different types of conferences.

Types of Conferences

The different types of conferences offer the following features:

	Ad-hoc	Scheduled	Permanent	Open
Usage	• Phone-controlled • application-controlled	• application-controlled	• application-controlled	• application-controlled
Start	• Manually	• Scheduled	• Manually	• Manually
End	• Manually	• Scheduled • Manually	• Manually	• Manually
Duration of the reservation of conference channels	• 1 hour by default	• Scheduled	• Until the deactivation or deletion of the conference	• Until the deactivation or deletion of the conference

	Ad-hoc	Scheduled	Permanent	Open
Extension	x	x	-	-
Recurrence	• Manually	• Scheduled	-	-
Direction of connection setup from the viewpoint of the system	• Outbound	• Outbound • Inbound	• Inbound	• Inbound
Set of participants	• Fixed	• Fixed	• Fixed	• Open
Authentication of conference participants	-	• Individual conference ID (optional) • Password (optional)	• Individual conference ID (optional) • Password (optional)	• Shared conference ID (optional)
Recording, if enabled in the system	• Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)	• Automatically (Auto Conference Recording) • Manually (On Demand Conference Recording)
Invitation by E-mail with:	• Conference Name • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password • Date and time of the start and end of the conference • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password • Link for Web Collaboration session	• Conference Name • Dial-in number • Conference ID • Password
Outlook appointment as an e-mail attachment (.ics)	-	x	-	-

Application-controlled Conference

As a subscriber, you can initiate, control and manage a conference with the Conference Management feature of myPortal for Desktop or myPortal for Outlook.

Phone-controlled Conference

As a subscriber, you can initiate a phone-controlled conference and then control it via the phone by the following methods:

- Call the desired conference participant and connect him or her to the conference
- Extend a consultation call into a conference

- Extend a second call into a conference

Virtual conference room

The virtual conference room enables you to follow a conference and its participants in a graphical environment (for application-controlled conferences) and to also manage the conference if you are the conference controller. The virtual conference room shows the phone number, name and presence status to the conference participants, where available.

Dial-in Number

As an administrator, you can change the conference dial-in numbers that were set up during basic installation. As a subscriber, you can display the dial-in number for a conference.

Conference Controller

The initiator of the conference is automatically the conference controller until this is explicitly changed. Depending on the type of conference, the controller can:

- Add or remove conference participants (for application-controlled conferences):

  Removed participants do not remain in the conference.
- Disconnect or reconnect conference participants:

  Disconnected participants remain in the conference. When the conference controller is connecting a conference participant, all other conference participants remain connected to one another. If there is only one participant connected, that participant will hear music on hold.
- Record a conference

  Recorded conferences are identified in the voicemail box with a red dot and show the call number of the first conference participant, if available. Conferences in which a participant is on hold cannot be recorded.
- Set another internal participant on the same node as the conference controller
- Extend the conference
- Leave the conference without ending it:

  The longest attending internal participant of the conference automatically becomes the conference controller.
- End the conference

Conference Participants

Conference participants can leave the conference and optionally dial-into it again (scheduled and permanent conferences). As long as a conference has only one participant, the participant hears music on hold. As an administrator, you can specify whether multiple external conference participants are allowed. The maximum number of external conference participants is determined, among other things, by the number of available trunks.

Conference tone

When connecting or disconnecting a conference participant, the other participants hear the conference tone. As an administrator, you can activate or deactivate the conference tone.

Automatic Termination without a Conference Controller

If there are only external subscribers left in a conference, the participants will hear an alert tone after a specified time period. Following a further timeout, the conference is automatically terminated by the system. As an administrator, you can edit these time values.

Notification by E-mail and Outlook Appointment

The system can automatically notify conference participants by e-mail and, for scheduled conferences, additionally through an Outlook appointment as an attachment (.ics):

Event	Notified conference participants	Outlook appointment
New conference	all	Automatic creation
Delete the conference		Automatic deletion
Reschedule the conference		Automatic update
Adding conference participants	Those affected	Automatic creation (those affected)
Remove conference participants		Automatic deletion (those affected)

This requires the administrator to have configured the sending of e-mails. In addition, an internal conference participant must have specified his or her e-mail address. For external conference participants, the initiator of the conference must enter their individual e-mail addresses.

NOTICE: For e-mail notifications, no return acknowledgments are obtained for failed deliveries or absence messages, since the e-mails are sent directly from the system due to the integration of Web Collaboration.

Further Calls

While participating in a conference, making a call or accepting another call disconnects the participant from the conference.

Park, Toggle/Connect

The Park and Toggle/Connect features are not available in a conference.

Call Charges

Toll charges are assigned to the party who set up the toll call. When a conference is transferred to another conference controller, all further charges are assigned to that controller.

System Load

As an administrator, you can display both active and saved conferences. Inactive conferences can be deleted.

INFO: Permanent conferences occupy system resources permanently. Since every subscriber can configure permanent conferences with myPortal for Desktop or myPortal for Outlook, you should, as the administrator, review the saved conferences regularly to avoid resource bottlenecks.

Video Monitoring

Any ongoing video transmission must be terminated before participating in a conference.

13.7.1.1 How to Change the Dial-in Number for a Virtual Conference Room

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Stations** in the navigation tree.
3) Navigate in the menu tree to **Stations** > **UC Applications** > **Conference**.

   The call numbers of the virtual conference room is displayed in the work area. The last of these is the one for scheduled and permanent conferences.
4) In the menu tree, click on the relevant entry (Index - Call number).
5) Click on the **Edit Station Parameters** tab.
6) Enter the new dial-in number in the **Phone Number** field. The dial-in number may only include the digits 0-9.
7) Click on **Apply** followed by **OK**.

13.7.1.2 Allowing or Preventing Multiple External Conference Participants

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **System Flags**.
4) Select one of the following options:
   - If you want to allow multiple external conference participants, enable the check box **More than 1 external conference member**.
   - If you want to prevent multiple external conference participants, clear the check box **More than 1 external conference member**.
5) Click on **Apply** followed by **OK**.

13.7.1.3 How to Activate or Deactivate the Conference Tone

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **System Flags**.
4) Select one of the following options:
   - If you want to activate the conference tone, enable the **Conference tone** check box.
   - If you want to deactivate the conference tone, clear the **Conference tone** check box.
5) Click on **Apply** followed by **OK**.

13.7.1.4 How to Change the Time Interval for the Automatic Termination of a Conference

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **Time Parameters**.
4) In the **Time until warning tone in main station interface transit connections** row, under **Base** and **Factor**, select the desired time period between the time the last conference controller leaves the conference and the alert tone.
5) In the **Time from warning tone until release...** row, select the desired time from the alert tone till the automatic termination of the conference.
6) Click on **Apply** followed by **OK**.

13.7.1.5 How to Check the Details of a Saved Conference

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Conferencing** wizard.
4) Click on the relevant user conference.
5) Click on **Display**.

13.7.1.6 How to Delete a Saved Conference

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Conferencing** wizard.
4) Click on the relevant user conference.
5) Click on **Delete** and confirm the security prompt.

13.7.1.7 How to Configure the Recording of Conferences

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Live Record**.
5) Select one of the following options:
   - 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) Click on **Save**.

NOTICE: Conferences that have this functionality activated cannot be transferred or held.

13.7.2 Ad-hoc Conference

An ad-hoc conference occurs spontaneously and is started manually by the conference controller. The conference controller can save ad-hoc conferences in order to set them up again at some later point in time.

Starting the Conference

The system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or myPortal for Outlook. The system calls all conference participants simultaneously. On joining the conference, each conference participant hears a greeting announcement with the name of the conference controller.

Recording the Conference

Conference controllers can record a conference manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via email. The duration of the recording is only limited by the available storage capacity of the system.

Ending the Conference

The conference controller can end the conference in the client or simply hang up. Alternatively, the conference ends when all conference participants have left the conference.

Expanding a Call to a Conference

An internal subscriber who is conducting a call can convert the call to an ad-hoc conference and add further subscribers. For this, the subscriber must have a UC Suite Conference license. This feature is not available for CallMe.

13.7.3 Scheduled Conference

A scheduled conference (Meet-Me conference) occurs at a pre-defined point in the future with a defined duration and may be set up to recur repeatedly at the same time.

A scheduled conference will run for the entire scheduled duration even if there are no connected participants. The conference controller saves a scheduled conference under a specified name.

Options for Configuring a Scheduled Conference

The initiator of the conference can define the following properties:

- Start time and End time
- Recurring conference
- Presence of conference controller required
- Authentication of conference participants on joining the conference required (by entering a conference ID and password via the phone keypad).

  NOTICE: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- Language of announcements before the conference begins
- Direction for the connection setup for each conference participant (default: **outbound**).

Starting the Conference

The system opens the window with the virtual conference room at the scheduled time automatically for all internal conference participants, provided they have started myPortal for Desktop with the classic user interface or

myPortal for Outlook. If the presence of the conference controller is required, the system first calls the controller. After the successful authentication of the controller, all the other conference participants are called simultaneously. Conference participants who have forwarded their calls to their voicemail boxes or who are determined to be absent by their presence status are not called. Depending on how the connection setup has been configured, the system calls the conference participants or the participants can dial in themselves. The system announces every participant who joins the conference by name, as in: "... has joined the conference", provided the initiator has recorded his or her name announcement.

NOTICE: Conference participants of a scheduled conference without authentication can only hear the announcement with the name of the conference controller at the start of the conference, provided they have already initiated a conference with authentication earlier on one occasion.

Dialing In

Every conference participant can use the dial-in number to dial into the conference within the scheduled time period, regardless of which direction for the conference setup was set for that participant. Attempts to dial into the conference outside the scheduled time period result in a corresponding announcement. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Forcing Authentication with the Star (*) Key

The conference controller can set the conference so that each conference participant is forced to provide authentication by at least by pressing the * key. This ensures that only the participants who are actually present are connected to the conference, as opposed to a voicemail box, for example.

Extending the Conference

Ten minutes before the scheduled end of the conference, the participants hear an announcement indicating that the conference is about to end and are offered the option of extending the conference by dialing a specific digit. Any conference participant can extend the conference by dialing that specific digit. The conference controller can extend the conference in myPortal for Outlook at any time.

Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

Ending the Conference

The conference ends at the time scheduled for the end of the conference or if the conference controller terminates the conference.

13.7.4 Permanent Conference

A permanent conference is not subject to time restrictions. The conference participants can dial in at any time.

The conference controller saves a permanent conference under a specified name. The conference is retained until it is explicitly deleted.

Options for Configuring a Scheduled Conference

The initiator of the conference can specify:

- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

  NOTICE: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- in which language the announcements before the start of then conference are to be made.

Starting the Conference

As soon as the first conference participant dials in, the system opens the window with the virtual conference room automatically for all internal conference participants, provided they have started myPortal for Desktop or myPortal for Outlook. All conference participants dial in themselves. The system announces every participant who joins the conference, as in: "`... has joined the conference.`"

Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Recording the Conference

Conference controllers can record a conference for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

An automatic recording of a permanent conference starts when there are two or more conference participants and stops when there are less than two participants. After the end of recording, all participants get the same record file for the complete conference.

13.7.5 Open Conference

Open conferences are intended for a fixed number of arbitrary participants. Any participant who has the requisite access data can dial into them.

The conference controller saves an open conference under a specified name. The conference is retained until it is explicitly deleted.

Options for Configuring an Open Conference

The initiator of the conference can specify:

- The number of conference participants (max. 16).
- whether the conference participants need to authenticate themselves by entering a conference ID and password via the phone keypad when joining the conference.

  NOTICE: Mobility Entry users must enter the code for DTMF suffix dialing before their authentication.

  The default password for conferences is 123456. The conference controller can change this for the conference participants individually.
- what common conference ID is valid for all conference participants.
- in which language the announcements before the start of then conference are to be made.

Starting the Conference

All conference participants dial in themselves. The system announces every internal participant who joins the conference, as in: `"... has joined the conference."`

Dialing In

Every conference participant can use the dial-in number to dial into the conference at any time. To dial in via an ITSP, the ITSP must support RFC 2833 (DTMF characters).

Recording the Conference

Conference controllers can record a conference automatically or manually for themselves or for all connected internal conference participants, provided the live recording of calls has been activated in the system. Participants located in the own node receive the recording in the voicemail box; participants in other nodes, via e-mail. The duration of the recording is only limited by the available storage capacity of the system.

13.8 Web Collaboration

The UC PC clients myPortal for Desktop (Windows) and myPortal for Outlook support the convenient integration of the separate product OpenScape Web Collaboration for simultaneous multi-media collaboration during phone calls and conferences. This provides quick access to functions such as desktop and application sharing, file sharing, co-browsing, whiteboarding, URL push, IM chat and video chat with multiple participants.

Web collaboration can be started by a subscriber during a phone call via the pop-up window of the UC PC client or by the conference controller of an active conference from within the conference. This opens the web collaboration session. A local installation of Web Collaboration on the UC PC client is not required. If an email program is available on the UC PC client, an email with the link to the web collaboration client can be sent to the communication partners. Detailed information on web collaboration can be found in the Web Collaboration product documentation.

When creating or editing a conference, the conference controller can also schedule a web collaboration session. On deleting or ending a conference, the associated web collaboration session is automatically deleted as well.

NOTICE: In order to enable UC PC clients to start web collaboration automatically, proxy authentication must be disabled whenever the UC PC clients access the Internet via a proxy server.

Supported Types of Connections

The web collaboration integration supports phone calls and phone-controlled conferences as well as the following types of application-controlled conferences:

- Ad-hoc conference
- Scheduled conference
- Permanent conference

Integration of Web Collaboration

For the integration of Web Collaboration, the address of the Web Collaboration server must be known to the communication system. The vendor offers the web collaboration server as a service on the Internet (Public Server). Alternatively, it may also be possible to use a Custom Server located on the customer's own network or with a partner. If the server is on the customer's own network, it is usually addressed by the communication system on TCP port 5004 using http. In the case of a hosted solution on the Internet (Public Server), a secure https connection is used instead, since the license number and password are transmitted over this connection. By default, TCP port 5100 is used for this purpose.

NOTICE: In order to use web collaboration, the communication system requires an Internet connection (default router and DNS server). Connections via proxy are not supported.

Internal conference participants with UC PC clients are automatically connected to the appropriate web collaboration session on starting the conference. To do this, a client is automatically downloaded and opened in the background, which may take several seconds. External conference participants with known email addresses receive an email with an appropriate link to the Web Collaboration session.

NOTICE: Users working under a MAC OS must close the alert dialog for the terminated session manually after completion of a web collaboration session.

For a scheduled conference, it is possible to connect to the Web Collaboration session as early as 5 minutes before the start of the scheduled conference.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages from a UC PC client do not appear in a web collaboration session of the same participant, and vice versa.

13.8.1 How to Configure the Connection to the Web Collaboration Server (Custom Server)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Internet access is available.

You need a license number and a password for the secure connection to the web collaboration server (custom server).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Web Services**.
3) Navigate in the menu tree down to **Web Services** > **Web Collaboration**.
4) Select the **Custom Server** radio button.
5) If you want to set up a secure connection to the web collaboration server (custom server), proceed as follows:
   a) In the **URL / IP address** field, enter the address of the web collaboration server (custom server) in accordance with the following pattern:

      `https://<URL Web Collaboration Server>:5100/xmlrpcsecure`

      or

      `https://<IP-Adresse Web Collaboration Server>:5100/xmlrpcsecure`
   b) Enter the license number for the secure connection to the web collaboration server (custom server) in the **Licence Number** field.
   c) Enter the password for the secure connection to the web collaboration server (custom server) in the **Password** field.

6) If you want to set up an unsecured connection to the web collaboration server (custom server), proceed as follows:
   a) In the **URL / IP address** field, enter the address of the web collaboration server (custom server) in accordance with the following pattern:

   ```
   http://<URL Web Collaboration Server>:5004/
   OscInterface
   ```

   or

   ```
   http://<IP-Adresse Web Collaboration Server>:5004/
   OscInterface
   ```

7) Click on **Apply** followed by **OK**.

13.8.2 How to Configure the Connection to the Web Collaboration Server (Public Server)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Internet access is available.

You need a license number and a password for the secure connection to the web collaboration server (public server).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Web Services**.
3) Navigate in the menu tree down to **Web Services** > **Web Collaboration**.
4) Select the **Public Server** radio button.
5) Enter the license number for the secure connection to the web collaboration server (public server) in the **Licence Number** field.
6) Enter the password for the secure connection to the web collaboration server (public server) in the **Password** field.

> **NOTICE:** If you want to test the Web Collaboration for 5 minutes, you can select the radio button **Public Server (Demo Mode/Evaluation Mode)**. No license number and password are required for this purpose.

7) Click on **Apply** followed by **OK**.

13.8.3 How to Disable the Connection to the Web Collaboration Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Web Services**.

3) Navigate in the menu tree down to **Web Services** > **Web Collaboration**.
4) Select the radio button **No Web Collaboration Server**.
5) Click on **Apply** followed by **OK**. The option to start a web collaboration session is disabled in the UC client.

13.9 Instant Messaging

Instant Messaging refers to communicating with instant messages (usually called a chat).

13.9.1 Instant Messaging

Instant Messaging enables you to chat with other peers. The system supports instant messaging with users of UC Smart, external communication partners and multi-user chats (or a combination of both).

Instant Messaging is possible with the following clients:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

As an administrator, you can enable or disable instant messaging on a system-wide basis. The sent and received instant messages are presented to the communication partners as an interactive dialog. On selecting a recipient, the client shows whether the communication partner is currently online. If one of the communication partners is offline, the following occurs with the instant message, depending on the type of the selected recipient:

Recipients	Behavior
Individual subscribers	The instant message is displayed at the next login.
Group in Favorites	The instant message is never displayed for the subscribers who are offline.

External Instant Messaging

As a subscriber, you can also chat with *one* external communication partner (e.g., a Google Talk user).

Multi-user chat

A multi-user chat is the exchange of instant messages with multiple communication partners. Here too, the system supports a maximum of one external communication partner.

Instant Messaging and Web Collaboration

Note that Instant Messaging of the system and Instant Messaging of a Web Collaboration session are mutually independent, i.e.: the instant messages

from a UC client do not appear in a Web Collaboration session of the same participant, and vice versa.

13.9.1.1 How to Enable or Disable Instant Messaging

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **General Settings**.
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.

   NOTICE: Disabling instant messaging has no effect on currently existing IM windows.
6) Click on **Save**.

13.10 AutoAttendant

Depending on the presence status of the called party, the AutoAttendant offers callers options to route voice calls to fixed numbers or their voicemail box. Callers signal their choice by entering digits at the phone.

13.10.1 Personal AutoAttendant

The personal AutoAttendant is the customized AutoAttendant, which can be configured by subscribers.

Personal AutoAttendant

As a subscriber, you can do the following for your station number with myPortal for Desktop or with myPortal for Outlook:

- Record or import announcements for the personal AutoAttendant.
- Configure profiles for the personal AutoAttendant

The relevant calls are first handled by the central AutoAttendant.

13.11 Voice and fax messages

The Voicemail and Fax services integrated in the system enable subscribers to receive and manage voicemails and fax messages via myPortal for Desktop and myPortal for Outlook. Fax messages can be sent by subscribers using Fax Printer.

13.11.1 Voicemail Box

The voicemail box records central voicemail and recorded calls. Subscribers can access it by phone and via UC Smart clients.

NOTICE: The default voicemail password can only be changed via an internal phone number.

Only voice messages longer than two seconds are recorded.

Managing Voicemail Messages

As a subscriber, you can listen to your voicemails:

- via a PC with myPortal for Desktop or myPortal for Outlook
- via your phone if your Presence status is **Office** or **CallMe**
- via any external telephone

Using myAttendant, the Attendant can also listen to voicemails of other subscribers who have explicitly allowed this.

The subscriber uses folders such as Inbox, Played, Saved or Deleted to manage incoming voicemail messages.

Voice messages can also be played back, paused and forwarded to another subscriber. The subscriber can also save voicemail messages in .wav format and redirect them to any selected email account.

The voicemail box can also be used by subscribers to manage recorded calls. Recorded calls are identified in the voicemail box by an appropriate symbol.

NOTICE: Information on the Phone menu can be found in the Quick Reference Guide documentation of the UC Suite Telephone User Interface (TUI).

Calling Back the Sender of a Voice Message

When listening to a voicemail, the subscriber can directly call back the person who left a message.

As an administrator, you can configure on a system-wide basis whether or not callbacks can be executed from the voicemail box

- from any phone number
- only from the own phone numbers of a subscriber configured under My Personal Details in the myPortal for Desktop, myPortal for Outlook, myAttendant and/or myAgent clients (**Extension**, **Mobile number**, **External Number 1**, **External Number 2**, **Private Number** and **Assistant Number**).

Retention Period

As an administrator, you can configure the retention period for voice messages.

Prioritizing voicemail messages

Callers can flag their voicemail messages as normal, urgent or private.

In myPortal for Desktop and myPortal for Outlook, the prioritization of existing voicemail messages is represented by different colors.

Subscribers who listen to their voicemail messages through the phone are first notified how many messages are urgent, private and normal. Urgent messages are played back first.

If the voicemail messages are forwarded as emails, the voicemails identified as urgent are flagged as emails with high priority.

Functionality of the Voicemail Box

The administrator can define the scope of the voicemail box. He or she can choose between:

- **Full**

  Full functionality of the voicemail box (default value)
- **Short Menu**
- After the status-based or personal announcement is made, a connection to the operator is offered.
- **No Menu**
- After the greeting announcement is played, the caller is directly taken to record a message.

Displaying New Messages at the Telephone

Voicemail messages are signaled at the telephone. As soon as the voicemail has been played, the indicators are deleted.

The type of signaling used for new voicemail messages depends on the phone

- For all telephones, acoustic signaling occurs using a special dial tone.
- For system telephones without a display, the Mailbox key also lights up (if configured).
- For system telephones with a display, the Mailbox key lights up (if configured), and a message appears on the display.

Notification Service

Subscribers who are using myPortal for Desktop or myPortal for Outlook can define whether the notification about the arrival of new voicemails should be forwarded and, if so, to what destination.

Subscribers can also define whether the message should be forwarded as an email. In addition, they can choose to be notified about the arrival of new voicemails by a phone call or an SMS.

Language of the Voicemail Box

As an administrator, you can select the default language of the voicemail box for the menu prompts and the internal system announcements on a system-wide basis.

Dependencies

Topic	Dependency
Playing a message over the phone	Subscribers can play back voicemails through the phone only in the **Office** or **CallMe** presence status. For all other settings, the message can only be played back via the PC.

13.11.1.1 How to Configure Station Numbers for Voicemail

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Setup** in the navigation bar.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click **Edit** to start the **Voicemail** wizard.
4) Enter the **VoiceMail Number**.
5) Click **OK & Next** followed by **Finish**.

13.11.1.2 How to Configure Call Forwarding to a Voicemail Box

You can use the **Call Forwarding** wizard to configure call forwarding for a subscriber to his or her voicemail box.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Call Forwarding** wizard. The **Configure the 'Call Forwarding - No Answer' feature** window appears.
4) Select the desired station in the **Select Station / Group** area.
5) Drag the **Voicemail box** with the mouse and drop it into the **Edit Call Forwarding** area.
6) If required, edit the time until call forwarding occurs (default: 15 seconds).
7) Click **OK & Next** followed by **Finish**.

13.11.1.3 How to Configure the Parameters of the Voicemail Box

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on the **VoiceMail** tab.
5) Select the language for the menu controls and the predefined announcements of your voicemail box in the **VoiceMail Language** drop-down list.
6) In the field **Voicemail Message Play Order**, specify in which order the messages should be played.
7) Enter the duration in seconds in the **Voicemail Message Recording Time** field.
8) Specify the scope of the voicemail box in the **VoiceMail Mode** field.
9) If you want callbacks to be executed from the voicemail box only to the call numbers that are entered in the UC clients under **My Personal Details**, select the check box **Allow callback from VM to known number only**.
10) If you want to switch off the last announcement which is played from the system, select the check box **Skip "please leave a message after the tone" prompt**. The system announcement will not be heard even if a professional record announcement is used.
11) Click on **Save**.

13.11.1.4 How to Configure Retention Periods for Voicemail

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Maintenance**.
5) Enter the respective retention periods in days in the fields under **Message**.
6) Click on **Save**.

13.11.1.5 How to Activate or Deactivate the Password Prompt for the Voicemail Box

Prerequisites

You are logged into the WBM with the **Expert** profile

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.

3) Click on **User Directory**.
4) Click on the relevant entry and then click on **Edit** > **Sensitivity**.
5) Click on **Security and Access**.
6) Select one of the following options:
   - If you want to activate the password prompt on calling your voicemail box, clear the **Bypass password when calling voicemail** check box.
   - If you want to deactivate the password prompt on calling your voicemail box, enable the **Bypass password when calling voicemail** check box.
7) Click on **Save**.

13.11.1.6 How to Configure an Info for Received Voicemails

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony Server** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click **Display** in the menu tree.
5) Enable the **Status display for info message** check box in the **Switches** area.
6) Click **Apply** followed by **OK**.

13.11.1.7 How to Configure a Mailbox Key to Check Voicemail

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Subscribers**.
3) Click **Edit** to start the **Key Programming** wizard.
4) Select the relevant station.
5) Select the relevant key in the first column.
6) Select the **Mailbox** function in the **Key feature** column.
7) Click **Apply** followed by **OK**.

13.11.2 Voicemail Announcements

Voicemail announcements notify callers about the Presence status of a subscriber, for example.

Standard announcements are available in all languages. As a subscriber, you can also record or import personal announcements for your voicemail box. The corresponding standard announcement is overwritten by the personal

announcement in the process. As an administrator, you can change the standard announcements by importing different announcements. The personal announcements of subscribers are overwritten in the process. The system performs the automatic level control and normalization needed to meet the "USA / TIA 968 Signal Power Limitations" requirements.

NOTICE: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

System Language for Voicemail Announcements

The system language for the voicemail box is set at the country initialization. In addition, the subscriber can set the language of his or her own voicemail box. A caller will then hear the station-specific announcements in the language set by the subscriber and the system-specific announcements in the system language.

Announcements Depending on Presence Status and Profile

Depending on the Presence status, the announcements for the voicemail box change automatically; for example, if the Presence status is **Meeting**, then the announcement may be something like: The subscriber is in a meeting until 3.00 p.m. today. If the entered end of a meeting is reached, but the subscriber has not yet changed his or her status back to "In Office", then the voicemail announcement is adapted automatically or the voicemail announcement reverts automatically to "In Office" (this is configurable by the subscriber).

The following table describes which greeting is heard by the caller, depending on the set Presence status and profile. The caller menu refers to the central AutoAttendant. The profile refers to the personal AutoAttendant of the subscriber here. The default greeting, name and custom greeting for profiles must be recorded by the subscriber. Depending on the configuration, the caller menu may vary in length or may not be available at all.

	Busy No answer Do Not Disturb	Meeting Sick Break Gone Out ...
Voicemail with Presence status	Default greeting + Caller menu	Name + Presence status + Caller menu
Voicemail box with blocked Presence status	Default greeting + Caller menu (if enabled)	
Profile with dynamic greeting	Custom Profile Greeting	Name + Presence status + Custom Profile Greeting
Profiles if dynamic greeting is to be skipped	Custom Profile Greeting	

If a subscriber has set his or her presence status to not be displayed to external callers, the external caller will always receive the "Busy" greeting for all presence states other than "Office" even if the called subscriber may not be actually busy in some cases. In this case, the subscriber should set up an announcement for the "Busy" greeting to indicate that he or she cannot accept the call.

13.11.2.1 How to Import Announcements for the Voicemail Box

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The audio files to be loaded are available as PCM files with the following properties: 8 kHz, 16 bit, Mono. The maximum length for the audio file name is 30 characters.

NOTICE: You can use the Audio Wizard to create audio files in advance, while mixing two sources, e.g., background music and announcements.

INFO: Before using announcements or music, make sure that you do not infringe on any copyrights.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **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) If you want to import an audio file, proceed as follows:

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) If you want to record an announcement using a phone, proceed as follows:

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**. The selected phone rings.

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 How to Change the Language for Voicemail Announcements

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **VoiceMail**.
5) Select the **VoiceMail Language** from the drop-down list.
6) Click on **Save**.

13.11.3 Fax Box

The fax box enables subscribers to receive and send fax messages via myPortal for Desktop or myPortal for Outlook without a fax machine.

As an administrator, you can configure a fax box for licensed subscribers. In addition, you can connect fax devices or fax servers via the a/b or ISDN interface.

As a subscriber, you can access your fax messages via myPortal for Desktop or myPortal for Outlook. myAttendant can access the fax messages of subscribers who have explicitly allowed this.

Managing Fax Messages

The subscriber can manage received fax messages by moving them to different folders (Saved or Deleted, for instance). The fax messages can also be forwarded to another subscriber. The subscriber can also save fax messages as PDF or TIFF files and redirect them to any selected e-mail account.

The administrator can configure whether the fax message is to be stored as a TIFF file (default) or as a PDF file on a system-wide basis.

NOTICE: To convert a TIFF file to a PDF file, the page size must be A4.

Retention Period for Fax Messages

The system automatically deletes fax messages for which the following retention periods are exceeded:

Fax message	Retention period (days)
New	120
Read	365
Sent	365
Deleted	60

13.11.3.1 How to Add a Fax Box for Stations

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Telephones/Subscribers**.
3) Click on **Edit** to start the **IP Telephones** wizard.
4) Click in the **Fax No.** field of the subscriber and enter the fax number under which the subscriber can receive fax messages (the preset hyphen must be deleted).
5) If a direct inward dialing number is to be configured for the fax box, click the **Fax Direct Inward Dialing** field and enter the Fax DID number (the preset hyphen must be deleted).
6) Click on **OK & Next**. If required, you can to print out a list of subscribers with the configured fax call numbers using **Print**.
7) Click on **OK & Next** and then **Finish** to complete the wizard.

13.11.3.2 How to Configure the File Type for Stored Fax Messages (UC Suite)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **General Settings**.
5) If you want to enable the saving of fax messages as PDF files, select the check box **Use PDF as fax format** in the **Fax Format** area.
6) If you want to enable the saving of fax messages as TIFF files, clear the check box **Use PDF as fax format** in the **Fax Format** area.
7) Click on **Save**.

13.11.4 Sending Fax Messages with Fax Printer

Fax Printer is an application for sending fax messages with centrally provided or individually created cover sheets from Windows applications such as Microsoft Word, for example.

Fax Printer consists of the following components:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer can be used from all the usual Windows programs. Fax groups make distribution easier. Fax messages are sent as an e-mail or directly to the Desktop. A screen pop notifies the subscriber when the fax is sent successfully.

Header Rows

As an administrator, you can configure different header lines for Fax Printer users. You can also define a header line as the default. Header lines may include the following elements:

Details	Placeholder
Date / Time	{{date_time}}
Company Name	{{company_name}}
User name	{{user_name}}
Company Ph.	{{company_number}}
Page number	{{page_number}}
Page count	{{page_count}}

The header lines of fax messages sent with Fax Printer may only include characters from the ANSI character set. In other words, no special or diacritical characters such as umlauts are allowed. Since the header line may basically include the sender's name, no special or diacritical characters should appear in the names of the subscribers as well.

13.11.4.1 How to Add a Central Cover Page

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

A fax cover page is available as a .opc file.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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) Select a .opc file.
7) Click on **Open**.
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) Click on **Save**.

13.11.4.2 How to Edit a Central Cover Page

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **File Upload** wizard.
4) Click on the **Central Fax Cover Page Upload** tab.
5) Click in the list of fax cover pages on the desired cover page.
6) Click on **Edit**.
7) Under **Name**, enter a name for the fax cover page.
8) Enter a **Description** for the fax cover page.
9) Click on **Save**.

13.11.4.3 How to Add a Header Line for the Fax Printer

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Fax Headlines** wizard.
4) Click on **Add**.
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. For each detail, a corresponding placeholder appears in the **Text** field.
7) To remove a detail from the header line, select the appropriate placeholder in the **Text** field, e.g., `{{page_count}}` (**Page count**) and press the `Del` key.
8) If required, enter any additional text in the **Text** field, e.g., "from" between the placeholders `{{page_number}}` (**Page number**) and `{{page_count}}` (**Page count**).
9) Click on **Save**.

13.11.4.4 How to Edit a Header Line for Fax Printer

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click on **Applications** > **UC Suite**.
3) Click on **Fax Headlines**.
4) Click in the list of fax headlines on the desired headline.
5) Click on **Edit**.
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. For each detail, a corresponding placeholder appears in the **Text** field.
8) To remove a detail from the header line, select the appropriate placeholder in the **Text** field, e.g., `{{page_count}}` (**Page count**) and press the `Del` key.
9) If required, enter any additional text in the **Text** field, e.g., "from" between the placeholders `{{page_number}}` (**Page number**) and `{{page_count}}` (**Page count**).
10) Click on **Save**.

13.11.4.5 How to Delete a Header Line for Fax Printer

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Fax Headlines** wizard.
4) Click in the list of fax headlines on the desired headline.
5) Click on **Remove**.

13.11.5 Notification Service for New Messages (UC Suite)

The system can optionally notify you (as a subscriber) about a new message by e-mail, by phone or with an SMS.

The Notification Service works as follows:

Notification	for voicemail	for fax message	Prerequisites
E-mail	You receive an e-mail with the message as a WAV file, the date and time it was received, the duration of the message and, if available, the phone number and name of the sender. If the size of the WAV file exceeds 10 MB (average 1MB/min), it is not attached to the e-mail. Voicemails with "urgent" priority are flagged as e-mails with "High" importance. E-mails with a voicemail have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	You receive an e-mail with the message as a PDF or TIFF file, the date and time it was received, the number of pages and, if available, the phone number and name of the sender. If the size of the PDF or TIFF file exceeds 10 MB, it is not attached to the e-mail. E-mails with a Fax message have a separate symbol in Outlook. If you are using an IMAP mailbox that shows only the e-mail headers, the usual e-mail icon will appear instead.	The delivery of e-mails has been configured in the system. The corresponding address is used as the sender.
SMS	You receive an SMS about the received message at the phone number defined by you.		The SMS template has been configured.
by phone	Your voicemail box calls you at the number you have specified and plays back the message to you.	-	

As a subscriber, you can enable or disable every type of notification for each Presence status individually. The notification by phone can be restricted to the business hours configured by the administrator. You can define the number and intervals for the repeated attempts for the notification by phone.

13.11.6 Sending E-mails

The feature for sending e-mails enables e-mail notifications about new voice and fax messages to be sent to subscribers and system messages to be sent to administrators by e-mail.

13.11.6.1 How to Configure the Sending of E-mails

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

An e-mail account with a password exists with an e-mail provider, and you know the access data for this account.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) Click **Service Center** > **E-mail Forwarding** in the navigation tree.

3) Enter the **Outgoing mail server (SMTP)** for the e-mail server to be used for sending e-mails, e.g., `smtp.web.de`. Ask your e-mail provider for the outgoing mail server if required.

NOTICE: In some cases, the sending of e-mails does not work because the name of the outgoing mail server cannot be resolved. To solve this problem, you must enter the IP address of the server instead of the name.

---

4) If a secure connection is required, enable the corresponding check box. If required, check with your e-mail provider whether this option needs to be enabled.
5) Enter the **User Name** of the e-mail account.
6) Enter the **Password** for the e-mail account and repeat it in the **Confirm Password** field.
7) Enter the **E-mail Address**, for example: `john.doe@web.de`.
8) If you want to now test the e-mail delivery, proceed as follows:
   a) Click on **Test Connection**.
   b) Under **Send to e-mail address**, enter the e-mail address of any e-mail box that you can access.
   c) Enter the **Subject** in the e-mail.
   d) Click on **Send Test E-mail**.
   e) Check whether you have received the e-mail.
   f) If the e-mail delivery failed, click **Back** and correct your e-mail settings (starting with step 3).
9) Enter the **E-mail Address 1** to get a notification email when ALI tolerance has been used. You may also enter a second email address.
10) Click on **OK & Next** followed by **Finish**.

Example

NOTICE: If you make configuration changes in the E-mail forwarding on an OpenScape Business X system with Booster Server you have to restart the Booster Server for the changes to take effect.

13.11.7 SMS Template

An SMS template enables subscribers to be notified about new voicemails with an SMS.

In order to receive SMS messages, a personal mobile e-mail address of the respective provider must be first activated. To do this, the subscriber sends an activation SMS to a speed-dial number. The subscriber then receives an SMS with his or her personal e-mail address, which is usually composed of the call number and the gateway name. For example, the mobile e-mail address for a T-Mobile customer with the phone number 0171/1234 567 would be: 01711234567@t-mobile-sms.de. This applies analogously to other networks as well.

An SMS template consists of the Template Details and SMS Details areas. The administrator must enter the name of the template in the Template Details area. This is usually the name of the E-mail-to-SMS Provider.

The specifications in the SMS Details area depend on the Provider. Under Recipient, the administrator must enter the e-mail address to which the SMS is to be sent. The entry for the Subject line may be freely selectable or require the customer number to be entered by the administrator.

NOTICE: Every Provider requires a specific template. The required data can be obtained from the respective mobile service provider.

Placeholder

SMS templates may include the following placeholders in the **Recipient**, **Subject** or **Text** field:

Details	Placeholder
Mobile number to which the message is to be sent	`{{MobileNumber}}`
Name or call no. of the sender	`{{Sender}}`
Date and time of receiving a message	`{{DateTime}}`
Caller number	`{{CallingNumber}}`
Priority of message	`{{Priority}}`

System-Specific Information

The length of the message is reduced to the first 160 characters.

13.11.7.1 How to Add an SMS Template

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Templates** wizard.
4) Click on **Add**.
5) Enter the **Template Name**.

NOTICE: The template name must not include any spaces.

6) Enter the name of the author under **Author Name**.

7) If you want to insert a placeholder, proceed in the following steps:
   a) Click in the field in which you want to insert the placeholder: **Recipients**, **Subject** or **Text**.
   b) Select the desired placeholder in the **VSL Fields** drop-down list.
   c) Click on **Insert**.
   d) If you want to insert additional placeholders, repeat step 7a-c accordingly.
8) Enter the **Recipient**.
9) Enter the **Subject**.
10) Enter the **Text**.
11) Click on **Create**.

13.11.7.2 How to Edit an SMS Template

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Templates** wizard.
4) Select the desired SMS template from the **SMS Provider** table.
5) Click on **Edit**.
6) Enter the **Template Name**.

   NOTICE: The template name must not include any spaces.

7) Enter the name of the author under **Author Name**.
8) If you want to insert a placeholder, proceed in the following steps:
   a) Click in the field in which you want to insert the placeholder: **Recipients**, **Subject** or **Text**.
   b) Select the desired placeholder in the **VSL Fields** drop-down list.
   c) Click on **Insert**.
   d) If you want to insert additional placeholders, repeat step 8a-c accordingly.
9) Enter the **Recipient**.
10) Enter the **Subject**.
11) Enter the **Text**.
12) Click on **Create**.

13.11.7.3 How to Remove an SMS Template

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Templates** wizard.
4) Select the desired SMS template from the **SMS Provider** table.
5) Click on **Remove**.
6) Click on **OK**.

13.11.8 Fax over IP (T.38 / G.711 Fax)

Fax over IP enables the transmission of fax messages over the Internet in accordance with the G2 and G3 standards by using the network protocol IFP (Internet Facsimile Protocol).

UC Suite can generally handle up to 8 simultaneous fax connections. Depending on the DSP module, OpenScape Business X3/X5/X8 as an ISDN gateway can handle from 3 to 12 concurrent faxes. Both parameters determine the number of simultaneous T.38 or G.711 fax connections.

NOTICE: It is highly recommended to use T.38 fax, if possible.

The system supports the following scenarios for T.38 or G.711:

- A subscriber receives fax messages via an ITSP (Internet Telephony Service Provider) at his or her fax box and sends faxes to external locations with Fax Printer via the ITSP.
- A subscriber receives fax messages via a Mediatrix 4102S (SIP) at his or her fax box and sends faxes with Fax Printer via a Mediatrix 4102S (SIP).
- Stations can receive Fax messages via an ITSP (Internet Telephony Service Provider) on a fax device that is directly connected to an analog or ISDN interface and send faxes from this fax device via the ITSP to external destinations.
- Stations can receive fax messages via an ITSP on a fax device that is connected to a Mediatrix 4102S and send faxes from this fax device via the Mediatrix 4102S and ITSP to external destinations.
- Stations can receive fax messages via ISDN on a fax device that is connected to a Mediatrix 4102S and send faxes from this fax device via the Mediatrix 4102S and ISDN to external destinations.
- A station can send fax messages from a fax device that is connected to a Mediatrix 4102S to another fax device that is also connected to a Mediatrix 4102S.
- Internal fax message from a fax device at an ISDN port to a fax device at a Mediatrix 4102S and vice versa.
- Internal fax message from a fax device at an ISDN port to a fax box and vice versa.

NOTICE: T.38 must be activated in the system for the fax box. In order to send faxes from the communication system via an ITSP, the ITSP must support T.38. In case the ITSP cannot switch to T.38, then the fax will be handled as G.711.

13.11.8.1 How Enable or Disable Fax over IP (T.38 Fax)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Voice Gateway**.
3) Click on **Voice Gateway** in the menu tree.
4) In the menu tree, click **Codec Parameters**.
5) Select one of the following options in the **T.38 Fax** area:
   - If you want to enable Fax over IP (T.38 Fax), select the **T.38 Fax** check box.
   - If you want to disable Fax over IP (T.38 Fax), clear the **T.38 Fax** check box.
6) Click on **Apply** followed by **OK**.

13.12 Microsoft Office 365 Integration Overview

You can work together easily with anywhere access to email, web conferencing, documents and calendars. It includes business-class security and is backed by Microsoft. Whether you are a small business or multinational enterprise, Office 365 offers plans designed to fit your organization;s unique needs. For more details or a 30 day account, please visit

OpenScape Business with Microsoft Office 365

When a user sets an appointment in their Microsoft Outlook calendar, the OpenScape Business system automatically checks for keywords in the calendar appointment subjects like: "meeting", "sick", "break, "out of office". If such a keyword is found, the system sets the user's presence status automatically when the appointment time is reached, even if Microsoft Outlook session of this user is not active anymore.

The user configures the appointments with these keywords and OpenScape Business sets the user's telephone presence status automatically and forwards the calls to the voicemail or, for example, to the cellphone, depending on the settings. The user can also configure in a general client status, if the presence status should switch to back to Office presence status when the appointment time is ended.

This also works even if the user does not use the local Outlook client and will set up an appointment with the above named keywords directly from the Outlook webpage in the cloud.

Email forwarding:

OpenScape Business is able to send emails to Microsoft Office 365 included Microsoft Exchange Server.

This enables the users to receive emails for new voicemails, faxes or conference calls with the ability to perform automatically Web Collaboration session from OpenScape Business .

OpenScape Business generates emails for such actions and keeps users updated also via email, if such new notification arrives in the OpenScape Business message box.

13.12.1 How to connect OpenScape Business system to Microsoft Office 365 using Basic Authentication

You can connect OpenScape Business system to Microsoft Office 365 in the cloud using basic authentication to use OpenScape Business Exchange Calendar Integration and Email Forwarding the integrated Microsoft Exchange Server in the Microsoft Office 365.

Prerequisites

- Microsoft Office 365- Office 365 Enterprise E3 with the known local installed " Microsoft Office Professional Plus" suite and the Office Web Apps usage.
- Users are available in Microsoft Office 365 and connected with the local Microsoft Outlook with the assigned email; addressed in Microsoft Exchange of Microsoft Office 365.
- All available Microsoft Updates and Service Packs are installed.
- Check out the right needed Microsoft Enterprise licenses.
- Check out the OpenScape Business Release Note for released Microsoft Office versions.
- Microsoft Office and the Office Web Apps needs to be installed locally.

Important notes:

- Change the value of the Microsoft Office 365 domain (example: test.onmicrosoft.com) to match your environment settings.
- The user "oso" is used in this example as Service Account with the role privilege for "ApplicationImpersonation" which is used to give the OpenScape Business access to the mailbox database of the Microsoft Exchange Server. This user has ti be added in the Microsoft Office 365 user directory as shown later. It requires also a configured email address.
- The known “Microsoft Exchange Public Folder Contacts search” of the Openscape Business Client is available, because Microsoft Office 365 offers this functionality.

Step by Step

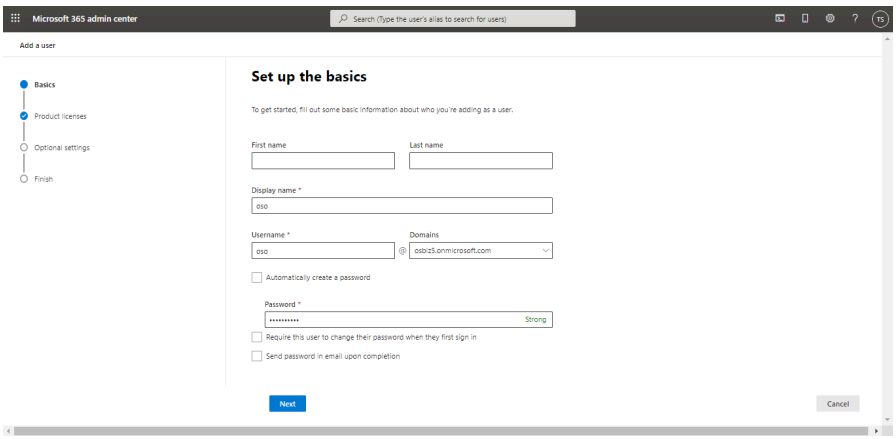
1) Register for **Microsoft Office 365 Enterprise E3** at the official web page of Microsoft.

a) Assign Global Administrator rights to user "oso".

2) Login to Microsoft 365 admin center and navigate to **Users > Active users** add the user "oso" and test users "user1- user3" and assign valid email addresses.

   Follow the setup wizard to configure the users.

   Add Global Administrator rights to user "oso".



3) Sign out from Microsoft 365 admin center and login with the new created user "oso" to change the temporary password.

   Check that user "oso" has access to the Admin page: **Health > Service Health**. After Service Health check is completed without any major issues sign out and login again with Microsoft 365 administrator again.

   Make sure that the users are available in the Microsoft Office 365 user directory and have already logged in to their profile once to change the temporary passwords and can login to their Microsoft Office 365 mailbox with the local installed Microsoft Outlook. This local Microsoft Office 365 installation has to be connected to Microsoft Office 365 portal and install and update it with all available Microsoft Updates for it.

4) Download Microsoft Office from Microsoft Office 365 portal, if not already done. Install and update it with the latest available Microsoft Updates.

5) Set the user "oso" as privilege user to be able to access the user calendars for the **Exchange Calendar Integration**.

   a) On a Microsoft Windows 10 computer open the PowerShell in elevated mode:

      - Open the start menu and type "Power" . The "Windows PowerShell command is marked.
      - Press and hold the Shift + Ctrl keys and use the Enter key to start the PowerShell.
      - Apply the upcoming UAC message with Yes to start the PowerShell.

   b) Check if the local execution policy allows script usage in the computer: `Get-ExecutionPolicy`

   c) If the result is not "RemoteSigned", then run the command: `Set-ExecutionPolicy RemoteSigned`. If that fails, check that the

privileges on this computer allow you to change this and have started the PowerShell in elevated mode.

d) Run the command lines to login to the online Microsoft Exchange Server and login with your main Microsoft Office 365 administrator account:

```
$LiveCred=Get-Credential Import-PSSession $Session -
AllowClobber
```

```
$Session = New-PSSession -ConfigurationName
Microsoft.Exchange -ConnextionUri https://
ps.outlook.com/powershell/-Credential $LiveCred -
Authentication Basic -AllowRedirection
```

```
Import-PSSession $Session -AllowClobber
```

e) Configure the Microsoft Office 365: `Enable-OrganizationCustomization`

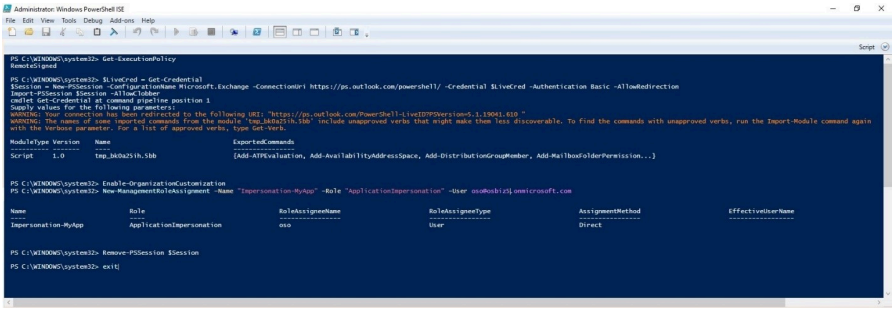
f) Change the privileged user value to match your environmental settings: `New-ManagementRoleAssignment -Name "Impersonatipon-MyApp" -Role "ApplicationImpersonation" -User oso@osbiz5.onmicrosoft.com`

g) Check the set value: `Get-ManagementRoleAssignment "Impersonatipon-MyApp"`

h) Leave the actual session: `Remove-PSSession $Session exit`

The PoweShell closes after the Exit command. If the PowerShell closes before the `Remove-PSSession $Session` is entered, then a new access may be locked for 15 minutes.

NOTICE: Ensure that the commands work and no red error messages are shown during the execution.



NOTICE: For more details about the PowerShell usage, see Microsoft Office 365 help.

---

6) Sign in to Microsoft Office 365 portal: www.office.com and log in with the user “oso” to get the information and select **Outlook** from the tree on the left. Then navigate to **Settings > View all Outlook settings > Mail > Sync email**.

Note down the server name and the port of the SMTP setting. For example, smtp.office365.com and 587. You will need this information for the next steps.

7) Navigate to **WBM > Setup > UC Suite > External Providers Config > Exchange Calendar Integration** and apply the following settings to connect with Microsoft Office 365 server:

   a) Click on the **Enable Exchange calendar integration** checkbox.
   b) From the **Authentication method** drop-down list, select **Basic**.
   c) Enter the **Server URL**. For example, https://outlook.office365.com/ews/exchange.asmx
   d) Enter the **Username** of the Privileged user set in Microsoft Office 365 directory.
   e) Enter the **Password** of the Privileged user password set in Microsoft Office 365 directory.
   f) Click **Save**.

   These changes will grant access of OpenScape Business to the Microsoft Exchange Server within the Microsoft Office 365 for the Exchange Calendar Integration.

   NOTICE: The fields for **Contact Providers > Exchange** must be filled with the online Exchange address: https://outlook.office365.com/ews/exchange.asmx and the email address of the global administrator (oso@osbiz5.onmicrosoft.com in this example), in order to be able to search contacts from public folders.

   ---

8) Navigate to **Service Center > E-mail Forwarding** to enable the mail access from OpenScape Business to Microsoft Office 365

   a) Enter the Microsoft Office 365 server address in **Outgoing Mail Server (SMTP)** field, the **Outgoing mail server port** and enable **This server requires an encrypted connection (TLS/SSL)** on **Server Information** area.
   b) From the **Authentication method** drop-down list, select **Basic**.
   c) Enter the **User Name, Password** and **Confirm Password** of the Privileged user in Microsoft Office 365 on the **Login Information** area.
   d) Enter the **E-mail Address** of the Privileged user in Microsoft Office 365 on the **User Information (Sender)** area.
   e) Enter the **E-mail Address 1** and **E-mail Address 2** in ALI change notification recipients area.
   f) Click **OK&Next**.
   g) Click **Check e-mail forwarding** to check that the function works.

9) Install the OpenScape Business client settings:

   As of February 2020, OAuth authentication is available for POP3, IMAP4, and SMTP AUTH connections to Exchange Online. So enabling authenticated client SMTP submission (SMTP AUTH) in exchange online is needed. Follow directions at: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

   Impersonation of the users is also needed. Log in with admin@osbiz5.onmicrosoft.com to office 365 and navigate to admin page on the left tree. New window tab will open. In the new window, under “Admin Centers” navigate to “Exchange”. New window tab opens again and under “Roles” on the left tree again, go to “Admin roles” tab and click “Add

role group". Give a name and press next. Click "ApplicationImpersonation" bullet and then "next". Finally add the users to the group and finalize.

Make sure that the Microsoft Office suite is installed to the user's computer and connected to Microsoft Office 365 and if not already done, install the CommunicationsClients with at least the option myPorta for Outlook.

a) Open the following path in Windows Explorer: \\198.6.127.12\applications\install-common\CommunicationsClients.exe

   Syntax: \\<Openscape Business ip-address>\applications\install-common\CommunicationsClients.exe

b) Login with WBM credentials and follow the setup wizard to install at least the option myPortal for Outlook.

10) Open Microsoft Outlook and login with the user's credentials to the OpenScape Business system with the OpenScape Business clients. For more details, see myPortal for Outlook user guide.

NOTICE: You can also use the **Silent Installation** option to install the CommunicationsClients unattended to the users computers. For more information, see Silent Installation/Uninstallation for UC Suite PC Clients on page 519.

---

11) Navigate to **WBM > Setup > UC Suite > User Directory** to add the user's email address.

OpenScapeBusiness will automatically send a "Welcome"-mail to all new entered mail-addresses with this configuration.

NOTICE: You can also perform this step in **WBM > Setup > UC Suite > User Directory**.

NOTICE: A configured valid mail-address is needed for the usage of the Exchange Calendar Integration and also for the optional mail notification when the user receives a message from OpenScape Business.

Repeat this step for all users.

12) Navigate to **WBM > Setup > UC Suite > Profiles** to configure the**Exchange Calendar Integration** feature.

a) Select the user you want to enable the feature, click **Edit** and then click on **My preferences > Outlook connectivity**.

b) Select the **Exchange Calendar Integration** option in the **Calendar integration**

c) Click on the **Automatically generate calendar appointments form my presence changes** checkbox

d) Select **Exchange PST** form the drop-down list.

Repeat this step for all users.

13) Navigate to **WBM > Setup > UC Suite > Profiles**. Select the user you want to configure and click on **VM Notification**, to configure if mail

notifications for voicemails will be sent in specific presence statuses, when a new voicemail is saved in the user's mailbox.

Repeat this step for all users. This step is optional.

14) Navigate to **WBM > Setup > UC Suite > Profiles**. Select the user you want to configure and click on **Fax Notification**, to configure if fax notifications for voicemails will be sent in specific presence statuses, when a new fax is saved in the user's mailbox

Repeat this step for all users. This step is optional.

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 How to check that Microsoft Office 365 Integration features are configured

E-Mail:

You can check the E-mail function with the button **Check e-mail forwarding** from the **Service Cente > E-Mail forwarding** area in WBM. Enter a valid mail addressas recipient and check receive of the test mail in the inbox of this mail account.

Exchange Calendar Integration:

When users set appointments in their Microsoft Outlook calendar, the OpenScape Business system automatically checks for keywords in the calendar appointment subjects like: "Meeting", "Sick", "Break", "Out of Office","Holiday","Lunch"or "Home". If such a keyword is found,the system sets the user's presence status automatically when the appointment time is reached, even if the Microsoft Outlook session of this user is not active anymore.The user simply configures the appointments with these keywords and OpenScape Business will set the telephone presence status automatically and will forward calls to the voicemail, or for example, to the cellphone, depending on the set presence status and the from the user desired forwarding target. The user can also configure in a general client setting, if the presence status should be switched back to "Office" when the appointmenttime ends.This will also work, even if the user does not use the local Outlook client and sets up the appointment with the above named subject keywords directly in the Outlook webpage in the Outlook Web Access (OWA).

The user that uses the Exchange or local Outlook Calendar integration must have a valide-mail address in their UC Suite client configuration as well as the

set UC Suite client Outlook settings configuration named in the manual above. It is madatory that the UC Suite-user to Exchange-user combination is done by the entered mail address,

The UC Suite users Voicemail language setting is used to combine the keywords like: "Meeting", "Sick","Break","Out of Office", "Holiday", "Lunch"or"Home" to the user's language setting, so for example if Geman language is selected in Voicemail, then German keywords will be checked in the appointments subject line like "Besprechung", "Krank", "Pause", "AuEer Haus", "Urlaub", "Mittag" or "Zu Hause" only.

If "Auto back to office" option is not used, the user's presence status will be kept to the set status after the appointment time ends and the return time shown other users or callers will be raised every 15 minutes. If the "Auto back to office" option is used and the appointment time ends, the user's presence is automatically set to "Office" again.

Appointments set into the future with less than 3 minutes are ignored, because the system expects that the user is just creating a new appointment there everything can change within these 3 minutes. The communication system checks for appointments in the users calendars every 30 seconds. For this reason and for possible time delays between the communication system and the Exchange Server, try to use test appointments with more than 3,5 minutes. In tests appointments set in to the future with more than 5 minutes works perfectly to avoid the small time delays between communication system and the Exchange server and the 30 seconds read delay of the calendar read requests.

New appointments values are fully read within the minute the appointment start time is set to within the before named 30 seconds queries. So in case start time is just reached, keep in mind that the 30 seconds query has to be done within this minute and then the presence status is set. The query also sets the users return time according to the end time of the appointment.

If you want to test the functionality when myPortal for Outlook or myPortal for Desktop is closed for the user, simply use the Outlook web page in the Outlook Web Access (OWA). Login with the users credentials and add the appointment with the keyword to the calendar. Check in another UC Suite user's client that the presence changes when the appointment time is reached.

14 Functions at the Telephone

The communication system offers a comprehensive set of telephony features extending from the usual features such as hold, toggle/connect and consultation hold, etc., through various call signaling mechanisms, down to call transfers, call deflections and call forwarding.

14.1 Making Call

The communication system offers many ways to make calls, including, among other things, direct station selection and speed dialing.

14.1.1 Digit Dialing

In the case of digit dialing, every digit is transmitted as soon as it is dialed.

The call setup begins immediately after the input of the first digit. Consequently, the subscriber has no way to edit the dialed number.

14.1.2 En-Bloc Dialing

In en-bloc dialing, connections are only established after the complete phone number has been entered. The call number is transferred as a single block.

The transmission of the dialed number can be initiated by entering the end-of-dialing code (#).

En-bloc dialing is mandatory for:

- ITSP trunk connection
- ISDN Primary Rate Interface in the U.S.

After 5 seconds without the input of a digit, the last entered digit is interpreted as the final digit of the number block.

14.1.3 Keypad dial

In some countries, the services of digital trunk connections are controlled using keypad dialing instead of functional control. To activate these services in the PSTN, you can use the stimulus interface.

The feature must be configured in E Manager.

Subscribers acknowledge the message traffic using the display. As a result, keypad dialing can only be performed on telephones with a display (optiPoint, OpenStage), mobile telephones (Cordless) with optiPoint menu navigation and IP telephones with stimulus interfaces. ISDN telephones are not supported. Each network provider determines which services can be used with keypad dialing.

An authorized station can activate keypad dialing using the service menu or using the *503 code. This is possible only in the idle state. Then the station must select an ISDN trunk that the feature can use.

Depending on the messages sent by the central office (such as when connecting), keypad dialing can create CDR entries. The number of the station using keypad dialing, the line used, and the time period when the feature was used are logged.

NOTICE: Actions triggered by keypad dialing are not monitored by the system. The system cannot prevent improper use, such as call charges fraud or trunk blocking.

Customers must be informed that they are liable for damages resulting from the improper use of this feature.

14.1.4 End-of-Dialing Recognition

End-of-dialing is either recognized automatically after five seconds or indicated manually by the user with the end-of-dialing code "#".

14.1.5 Editing the Telephone Number

This option lets subscribers modify the digits entered for the station number. This function is common in mobile phones. A call number can only be corrected as it is being entered.

After entering a sequence of digits, the user can edit it from right to left by pressing a key; each time the key is pressed, one digit is deleted. Once the correct digit sequence is entered in full, the user can press the confirm key or lift the handset to start digit transmission.

It is not possible to edit a saved call number, for example, for number redial.

INFO: This feature can be individually activated for every station.

Dependencies

Topic	Dependency
Call waiting	Call waiting is possible during editing because the telephone is in digit input state and is busy for incoming traffic.
Consultation	The telephone is in digit input state after a consultation. This makes it possible to edit station number digits.

14.1.5.1 How to Activate or Deactivate Editing of the Telephone Number

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) In the menu tree, click the station (Index - Call number - Name).
5) Click on the **Edit Station Flags** tab.
6) Select one of the following options:
   - If you want to activate the function, select the check box **Edit tel. number**.
   - If you want to deactivate the function, clear the check box **Edit tel. number**.
7) Click on **Apply** followed by **OK**.

14.1.6 Redialing

The phone number dialed is saved after an external call is set up. If the destination is busy or not reachable, a user can press the Redial key to redial the same number.

Speed dial numbers are also stored in the redial memory.

Dialing internal call numbers has no effect on the redial memory.

Post-dialed digits (also called DTMF characters), if any, are not seen as part of the dialing information and are therefore not saved (e.g., digits sent to a connected voicemail box).

The Redial function can only be activated via a key, not via an access code.

To retrieve a specific number and use it to set up another call, press the Redial key. Press the key once to dial the last number dialed. Press the key twice to dial the next-to-the-last number dialed. Press the key three times to dial the number that was stored the longest.

The station number saved is automatically dialed after 2 seconds when you press the Redial key. If you need more time to read the displayed station number, select "scroll" with the Confirm Key. Click "Next" to display the next phone number saved. This is phone number is dialed only on selecting the "Make Call" command. This gives you much more time to check if the correct phone number was selected.

In the case of a call routed via LCR, only the number dialed by the station is stored.

Account codes are also stored in the redial memory. This is true only if the appropriate system-wide flags are set.

14.1.6.1 How to Enable or Disable Automatic Redialing

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **System Flags**.
5) Select one of the following options:
   - If you want to activate the function, select the check box **Automatic redial**.
   - If you want to deactivate the function, clear the check box **Automatic redial**.
6) Click on **Apply** followed by **OK**.

14.1.7 System Speed Dialing

You can save frequently needed external phone numbers in the communication system. Every number is then represented by a speed-dial number which is used instead of the full phone number.

Speed-dial numbers consist of 4-digit numbers.

All subscribers are members by default of a group that is assigned all SSD numbers. This means that every subscriber can use all SSD numbers.

SSD overrides toll restriction rules. Note that dialing a speed dial destination found during a search in the internal phonebook will not override toll restriction rules.

The numbers for system speed dialing are configured by the administrator in groups. The subscribers can each be assigned to one of these groups. A subscriber can only use the speed-dial numbers of his or her allocated group. A group can only be assigned a single SSD range.

Entries in speed dials are searchable by first and last name if name is configured in <Last Name>, <First Name> or <First Name>, <Last Name> format.

Used speed dial numbers are stored in the redial memory.

To program a "dial pause" and DTMF changeover for suffix dialing of DTMF characters (e.g., for controlling voicemail boxes), you can use the Repdial "P-key" or "#" (pound) key.

The repdial key for the customer must be set as:
<dial_number><dtmf_digit><pause_digit><access_code> e.g. 008007728477#P2210344

Translation of station numbers to names

You can assign a name to each speed-dialing destination. As soon as a call is received from a saved phone number, the system automatically enters the name and displays it instead of the phone number if CLIP is set.

Suffix-dialing

Suffix-dialing is not supported for "en-bloc sending" Digit Transmission (e.g., an ITSP configuration). It is supported for "Digit-by-digit" Digit Transmission.

NOTICE: Digit trasmission field can be changed in WBM via **Expert mode > Trunks/Routing > Route**

Suffix-dialing is also possible:

- Manual suffix-dialing

  The user can select additional numbers by selecting the access code and entering the index number (speed-dial number). These are added to the station number saved in this index and dialed.
- Automatic suffix-dialing

  When configuring an SSD, the number entered can be split into two parts. A dash "-" is used as the separator. The first part is always sent. A timer then starts. If the user does not dial any more digits before the timer expires, the second part of the number entered is automatically suffix-dialed, otherwise the manually dialed digits are transmitted.

  For example: SSD = 7007–0

  If the station does dial a DID (manual suffix-dialing) after selecting the SSD and before the specified time has expired, 0 is automatically dialed (automatic suffix-dialing).

Importing Speed Dial Numbers

You can import speed-dial lists from an XML file in UTF-8 format. Existing speed dial numbers are deleted before the import.

An XML template with the appropriate explanations can be found in the WBM under **Service Center** > **Documents** > **CSV Templates**. You can enter your speed dial destinations in these templates by using Microsoft Excel, for example.

NOTICE: Import of speed-dial lists from CSV files is not recommended any more and it's only supported in special cases.

Exporting Speed Dial Numbers

As an administrator with the **Expert** profile, you can export speed-dial numbers to an XML file in UTF-8 format in the **Expert mode**. The export always includes all the records.

14.1.7.1 How to Add a Speed Dial

The **Phone Book/Speed Dialing** wizard can be used to add speed-dial destinations for system speed dialing.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Phone Book/Speed Dialing** wizard.
4) Enter the **Speed dial** number, the **Call number**, and the **Name** of the speed-dial destination in a free table row.
5) If you want to add further speed-dial destinations, click on **Store data** and repeat the previous step.
6) Click on **OK & Next**.
7) Click on **Finish**.

14.1.7.2 How to Import Speed Dials from an XML File

The **Phone Book / Speed Dialing** wizard can be used to import speed-dial numbers and phone numbers from an XML file. Existing speed dial numbers are deleted before the import.

Prerequisites

You are logged in at the WBM.

An XML file with the entered speed dial numbers is available in UTF-8 format. An XML template for importing speed-dial numbers can be found under **Service Center** > **Documents** > **CSV Templates**.

NOTICE: Import of speed-dial lists from CSV files is not recommended any more and it's only supported in special cases.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Phone Book/Speed Dialing** wizard. The **Edit central phone book** window appears.
4) Click on **Import/Export CSV/XML Data**.
5) Click in the **Import CSV/XML file via HTTP** area on **Browse** to select the desired file.
6) Click on **OK**. Existing speed dial numbers are deleted, and the speed dial numbers entered in the XML file are imported into the system.
7) Click on **Finish**.

14.1.7.3 How to Export Speed Dials to an XML File

You can export speed dial numbers to an XML file. The export always includes all the data.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Phone Book/Speed Dialing** wizard. The **Edit central phone book** window appears.
4) Click on **Import/Export CSV/XML Data**.
5) Click in the **Export XML file via HTTP** area on **Download**. The list of speed dial numbers is prepared for downloading.
6) Select the storage location for the file and click **Save**.

14.1.7.4 How to Edit Speed Dials

The **Phone Book/Speed Dialing** wizard can be used to edit speed-dial destinations.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click **Edit** to start the **Phone Book/Speed Dialing** wizard.
4) You can search for an entry by typing a search term in the **Speed dial**, **Call number** or **Name** search fields and then pressing the return key. All matches that contain the search term are displayed. For example, entering the call number `521` would display the matches `+495213535` and `+498967521`, and entering the term `co` as the name would display `Collins`, `Mcoin` and `Branco`.

   NOTICE: Pressing the return key with nothing entered in any of the search fields causes all entries to be displayed.

5) Edit the values for the desired table entry in the **Speed dial**, **Call number** or **Name** fields.
6) If you want to edit additional speed-dial destinations, click on **Store data** and repeat the previous step.
7) Click **OK & Next**.
8) Click **Finish**.

14.1.8 Individual Speed Dialing (ISD)

Individual Speed Dialing (ISD) enables every subscriber to save 10 external numbers as individual speed-dial numbers in addition to the system speed-dial numbers.

For telephones without a display, the station user must wait for the confirmation tone following station number entry.

External numbers can be programmed in the ISD pool. Access depends on the station's dial-up access rights. Before entering the station number, the subscriber must enter the CO access code (e.g., 0).

The Redial key or the pound (#) key is used to program a dial pause or DTMF changeover.

14.1.9 Direct station select

The function keys on a telephone or add-on device can be programmed as DSS keys. These are programmed with the phone number of an internal subscriber or a group for this. Press a key of this kind to initiate an immediate call to the programmed destination (DSS). The current status of the subscriber or of the group is indicated by the LED associated with the DSS key.

A DSS (direct station selection) key can also be used to transfer a call quickly to the programmed subscriber or group. Pressing a DSS key during a call with an external party places the ongoing call on consultation hold. The transferring subscriber can transfer the call to the transfer destination by replacing the handset (unscreened transfer). He or she can also wait until the transfer destination responds before transferring the call (screened transfer). If the transfer destination does not answer, an automatic recall is enabled.

Statuses of a DSS Key LED

The DSS key LED shows the current status of the programmed station:

- Off: the associated subscriber is not conducting a call.
- Lit: the associated subscriber is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated subscriber is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated subscriber is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Dependencies

Topic	Dependency
ISDN phones, SIP phones	Direct Station Select (DSS) keys cannot be programmed for ISDN or SIP telephones.

Related concepts

Team Configuration / Team Group on page 672
Executive/Secretary or Top Group on page 676

14.1.10 Speaker Calls / Direct Answering

The Speaker call function lets you set up an internal connection without the called subscriber lifting the handset. The loudspeaker on the called station is automatically activated.

On phones equipped with a speakerphone (microphone), direct answering of the called station is possible by switching on the microphone. On lifting the handset, the call becomes a normal two-party call.

Speaker calls can be used via a function key programmed for this purpose, the associated menu item or by entering the code and then dialing the station number of the destination station or group. A function key can also be programmed with a station number. A connection to the programmed destination is immediately set up when you press a function key of this kind.

Speaker calls also enable the broadcasting of announcements to all internal members of a group.

Direct answering can be activated via the menu item provided for this in the display or via a function key programmed for this purpose.

Speaker calls can be prevented for a subscriber by enabling an option to prevent voice calling. In this case, speaker calls are signaled like a normal call.

Dependencies

Topic	Dependency
Do Not Disturb, Override Do Not Disturb	Speaker calls are not possible at stations where Do Not Disturb is active. If the subscriber who wants to use the "Speaker calls" feature is authorized to override Do Not Disturb, he or she hears the busy tone for five seconds. The destination station is then called, but not directly addressed.
Toggle, consultation hold, transfer	The specified features cannot be used in a speaker calls/direct answering connection.
ISDN phones, SIP phones	The "Speaker call" and "Direct answering" features cannot be used with ISDN or SIP telephones.

14.1.10.1 How to Enable or Disable the Prevention of Speaker Calls for Stations

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) Navigate in the menu tree under **Stations** > **Station** > **…** down to the desired station (Index - Station Number - Name).
4) Click on the **Edit Station Flags** tab.
5) Select one of the following options:
   - If you want to enable the prevention of speaker calls for stations, clear the check box **Prevention of voice calling off**.
   - If you want to disable the prevention of speaker calls for stations, select the check box **Prevention of voice calling off**.
6) Click on **Apply** followed by **OK**.

14.1.11 Associated Dialing

Associated dialing enables an authorized subscriber to dial a phone number on behalf of any other subscriber. The effect is the same as when the other subscriber dials the phone number.

The user accesses the function by dialing a code and specifying the station for which a number should be dialed. The system then interprets this information as though the station specified earlier were dialing.

14.1.12 Trunk Queuing

A subscriber can reserve a trunk in advance if there are no free trunks available (busy signal). As soon as a trunk becomes free, it is offered to the subscriber through an automatic recall.

If the user is busy at the time of the recall, the trunk will camp on to the busy station. If the camp-on tone is not answered, the reservation is canceled, and the trunk is offered to the next station in the queue. If the user activated DND prior to receiving the recall from the queued trunk, the trunk reservation is canceled and the trunk is offered to the next station in the queue.

If a number of stations queue a trunk, the trunk is assigned in the order that the requests were received.

Only one queue/reservation request is accepted per telephone. If a second reservation is attempted, it overwrites the first.

It is not possible to invoke the Trunk Queuing feature if the attempted call was placed through LCR (least cost routing).

The Trunk Queuing feature ignores an existing call forwarding—no answer instruction. Trunk reservation is canceled if not answered within 20 seconds.

A recalling trunk cannot be picked up by either Call Pick up - group or Call pick up - Directed.

Trunks can be reserved in one of the following ways:

- Manual reservations only work in telephones with a display
- Automatic reservation (for all other telephones)

  When this flag is activated and if a station is not assigned a free trunk after the usual simplified dialing procedures, the busy tone is signaled at the station. After five seconds, a positive acknowledgment tone is applied and the trunk is reserved, provided that the station has the appropriate CO call privilege.

NOTICE: Trunk queuing is not possible for S_0 phones.

14.1.12.1 How to Activate or Deactivate Trunk Queuing

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **System Flags**.
5) Select one of the following options:
   - If you want to activate the function, select the check box **Trunk reservation, automatic**.
   - If you want to activate the function, clear the check box **Trunk reservation, automatic**.
6) Click on **Apply** followed by **OK**.

14.1.13 Private Trunk

A private trunk is a CO trunk that is available exclusively to a specific subscriber.

14.2 Call Signaling, Calling Line ID

The communication system offers various options for call signaling and call number display such as CLIP, CLIR, COLP and COLR, for example.

14.2.1 Different Call Signaling

Different call signaling enables a distinction to be made between internal and external incoming calls.

Incoming calls are signaled visually and acoustically on the phone. The following displays appear on the screen:

- Caller number
- For internal call forwarding: additionally, the dialed call number

The incoming call can also be signaled via an LED. Different acoustic signals are used for internal and external calls.

Call signaling internal

Each subscriber can be assigned one of a total of eight possible acoustic call signals for internal calls. The station then uses the modified ringing tone to distinguish its calls at other internal stations. For example, a special internal ringing tone can be set for the manager so that every staff member knows when the manager is calling simply from the ringing tone.

Call signaling external

There are three different call types, each with different acoustics, that can be set for an external call. Different acoustic signals can be applied, for instance, to distinguish between calls from two different groups such as Sales and Warehouse.

- In Germany, the administrator can configure three different ring types for analog, ISDN and system phones.
- In other countries, the ring types for analog phones are the same.

14.2.2 Calling Line Identification Presentation (CLIP)

Calling Line Identification Presentation (CLIP) shows the caller's number at the called station.

The CLIP (Calling Line Identification Presentation) refers to incoming calls and must be supported by the network provider.

If the caller's name and phone number are programmed as a system speed dialing (SSD) number in the communication system, you will see the name on your display.

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

Configurable CLIP

Configurable CLIP transmits a set call number (e.g., the call number of a hunt group) externally instead of the caller's number (e.g., the number of the hunt group member).

System-Specific Information

Country	Enabled by default
USA	LIN (Location Identification Number). If CLIP is enabled for the USA, LIN is automatically disabled.
Remaining countries	CLIP

14.2.2.1 How to Enable or Disable Configurable CLIP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **System Flags**.
5) Select one of the following options:
   - If you want to enable Configurable CLIP, select the **Configurable CLIP** check box.
   - If you want to disable Configurable CLIP, clear the **Configurable CLIP** check box.
6) Click on **Apply** followed by **OK**.

14.2.3 Calling Line Identification Restriction (CLIR)

Calling Line Identification Restriction (CLIR) suppresses the station number of the caller at the station of the called subscriber.

CLIR (Calling Line Identification Restriction) applies to outbound calls. The PSTN must support the feature. The Calling Line Identification Restriction (CLIR) has precedence over the Calling Line Identification Presentation (CLIP).

The Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) features are mutually exclusive, that is, as soon as CLIP is activated, CLIR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

Calling Line Identification Restriction (CLIR) has no effect for certain call destinations (e.g., emergency numbers of the police and fire departments).

System-wide Station Number Suppression (CLIR)

As an administrator you can enable or disable the CLIR station number suppression on a system-wide basis.

INFO: The flag "System-wide station number display suppression" does not apply to the U.S.

Temporary Station Number Suppression

As a subscriber, you can activate or deactivate the temporary station number suppression (CLIR). A temporary station number suppression is only possible if the system-wide station number suppression has been deactivated.

Station Number Suppression (CLIR)

As an administrator, you can configure the CLIR for each route so that only the PABX number is transmitted instead of the subscriber's station number.

14.2.3.1 How to Enable or Disable Station Number Suppression

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) Select the corresponding **Trk Grp.**.
5) Select the check box **Suppress station number** under **System number - outgoing**.
6) Click on **Apply** followed by **OK**.

14.2.4 Connected Line Identification Presentation (COLP)

Connected Line Identification Presentation (COLP) transmits the call number of the called subscriber to the caller as soon as the two are connected.

COLP makes sense with call forwarding, for example, so the caller can see the phone number of the actual communication partner instead of the originally dialed phone number.

The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

14.2.4.1 How to Enable or Disable Connected Line Identification Presentation (COLP)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) Select the appropriate **Trk Grp.**.
5) Click on the **Special Parameter change** tab.
6) Select the check box **COLP**.
7) Click on **Apply** followed by **OK**.

14.2.5 Connected Line Identification Restriction (COLR)

Connected Line Identification Restriction (COLR) suppresses the display of the called station at the station of the caller.

The Connected Line Identification Restriction (COLR) applies to incoming calls.

The Connected Line Identification Restriction (COLR) has precedence over the Connected Line Identification Presentation (COLP).

The Connected Line Identification Presentation (COLP) and Connected Line Identification Restriction (COLR) features are mutually exclusive, that is, as soon as COLP is activated, COLR is deactivated, and vice versa.

CLIR and COLR can only be enabled or disabled together.

14.2.6 CLIP No Screening (Transmission of Customer-Specific Phone Number Information)

CLIP No Screening transmits a call number specified by the caller instead of the caller's own number.

The outgoing system number does not have to be identical to the incoming system number.

The "Suppress station number" flag can be activated for special customer applications. This prevents the system from sending out the DID number of the station along with the outgoing system number.

Example: You want to prevent direct customer access to a service staff member who is reached centrally with a general service number. To conceal the staff member's own DID number, enter the general service number as the outgoing PABX number and activate the "CLIP no screening" flag. Then called subscribers see only the general service number on their display as the CLIP.

Incoming and outgoing calls usually use the same system number. In this case, the entry under "System number - outgoing" is either empty or the same as the one under "System number- incoming". If this is not the case, you can

- enter a different number under "System number - outgoing".
- use the routing parameter "No. and type, outgoing" to define whether the "System number - outgoing" entered contains the station number without area code, with area code (national), or also with the international country code (international).

INFO: CLIP no screening must be supported by the Network Provider and be activated.

14.2.6.1 How to Configure CLIP No Screening

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) Select the corresponding **Trk Grp.**.
5) Enter the required **PABX number** under **System number - outgoing**.
6) Click on **Apply** followed by **OK**.

14.2.7 CLIP for Analog Telephones

CLIP for analog telephones transmits the call number of an analog device of the caller to the called party and displays the CLIP (Calling Line Identification Presentation) on suitable devices of the called party analogously.

The additional transmission of CNIP name information (Calling Name Identification Presentation) can be configured.

INFO: CNIP is device-independent. Please also refer to the vendor specifications.

14.2.8 Ringer Cutoff

The Ringer Cutoff feature signals incoming calls acoustically with only a brief alert tone (beep) and on the display.

Ringer Cutoff is only available on phones with displays and has no effect on the signaling of appointments.

14.2.9 Translating Station Numbers to Names for System Speed Dialing

For calls made using system speed-dials (SSD) and for incoming calls from system speed-dial numbers, the name associated with the speed-dial destination is displayed after dialing instead of the speed-dial number.

14.3 Functions During the Call

The communication system offers several functions during calls, e.g., holding, redirecting and transferring calls.

14.3.1 Placing a Call on Hold

Placing a call on hold causes the call to be held in a waiting state. During this period, the caller usually hears an announcement or music on hold.

The hold ends when the held call is retrieved (i.e., resumed).

The following types of holds are possible:

- Common hold:

  Any subscriber can retrieve the call again by pressing a trunk or call key
- Exclusive hold: (only for Team or Top function and at the Attendant Console)

  Only the initiating party can retrieve the call.

Placing a Call on Hold and Automatic Recall

A parked call results in an automatic recall when the **Time for parking + change to hold** timer expires (default: 160 s).

14.3.2 Parking

Parking a call causes that call to be placed in a waiting state. During this period, the caller usually hears an announcement or music on hold. A parked call can be retrieved from any telephone.

As a subscriber, you assign a park slot (0-9) for a call to be parked. If the park slot you select is already occupied, a negative confirmation tone sounds and the number does not appear on the screen. You can then select another park slot. To retrieve a parked call, you must specify its park slot.

A parked call can be retrieved (unparked) via a code or a correspondingly programmed key and can also be retrieved if another call is waiting at the same time.

Parking and Automatic Recall

A parked call results in an automatic recall when the **Time for parking + change to hold** timer expires (default: 160 s).

Parking and Call Forwarding

In the case of a recall, a parked call does not follow call forwarding.

Parking and DISA

Parking cannot be enabled via DISA.

Parking and Conference Calls

You cannot park a conference call.

Parking and Networking

A parked call can only be retrieved in the same node. An incoming call over a network can only be parked at the destination node.

Parking and Do Not Disturb

A station with DND enabled can place a call in a park slot; however, if a recall occurs from the parked call, and no other destination was defined in the call management, the call will be automatically disconnected after the recall timer expires.

NOTICE: Detailed instructions on how to park a call and how to retrieve a parked call can be found in the relevant chapter of the corresponding device's user guide (OpenStage X Hipath/ OpenScape 3000/ 4000 User Guide).

14.3.3 Consultation

In the case of a consultation hold, a subscriber initiates a second call from the same phone or accepts a waiting call. In the meantime, the first call is placed on hold.

A consultation hold is terminated on:

- retrieving the held call or
- Disconnect

  This results in either:

  – a transfer of the held call or
  – an immediate automatic recall from the party on hold to the party that has just hung up

Consultation Call using the Direct Station Select (DSS) Key

Pressing a Direct Station Select (DSS) key during a call initiates a consultation call to the corresponding destination.

Connecting two External Parties

During an external call, a consultation call to another external destination followed by a transfer connects the two external parties. This may involve call charges.

14.3.4 Toggle/Connect

The Toggle/Connect feature enables a subscriber to switch between two calls. When the subscriber is talking to one party, the other party is placed on hold.

The subscriber can toggle between the two calls by pressing the appropriate trunk key.

Toggle/Connect and Placing a Call on Hold

The Toggle function is not available to an on-hold subscriber.

14.3.5 Transfer

A transfer enables a subscriber to transfer his or her call to another destination. As soon as a subscriber initiates a transfer, the waiting party is placed on hold for the time being.

The following types of transfers are possible:

- Blind transfer (also called an unscreened transfer):

  You can transfer the call without an answer from the subscriber at the destination of the transfer. If the station at the transfer destination is busy, the call is camped on (i.e., call waiting is signaled). If a third party now tries to transfer a call to this busy station or if call waiting rejection has been turned on at the transfer destination, an immediate recall occurs. If the subscriber at the transfer destination does not accept the transferred call within a specified time period ("Dial time during transfer before answer" timer), an automatic recall occurs. A blind transfer (also called an unscreened transfer) to an agent in another Multimedia Contact Center queue is not possible.
- Consultation transfer:

  You can transfer the call only if the subscriber at the destination of the transfer answers. The transfer is completed by hanging up the handset.

Transfer with Call Forwarding

Any call forwarding set at the transfer destination will be followed, i.e., the call will be forwarded accordingly. The display shows the final destination of the transfer.

Transfer with Do Not Disturb

Transferring a call to a station at which Do Not Disturb is enabled results in an immediate recall to the transferring station even if the transferring station itself also has Do Not Disturb enabled.

System-Specific Information

"Dial time during transfer before answer" timer: 45 seconds by default

Up to 5 calls can be transferred simultaneously to a busy station.

NOTICE: In a call transfer, the display information update through the ITSP/NATIVE-SIP interface is not supported.

14.3.6 Automatic Recall

An automatic recall is received by the originator of a call if his or her call was placed on hold or parked for too long or if an attempt to transfer that call was unsuccessful.

An automatic recall occurs in the following cases:

- A held or parked call is not picked up again within a specific time period ("Time for parking + change to hold" timer).
- In the case of unscreened transfers, under the following circumstances:
  - The call is not answered before a certain time period expires ("Dial time during transfer before answer" timer)
  - The destination does not exist
  - The destination is busy with a second call
  - The digital phone at the destination is defective
  - The transfer type is not allowed

If the originator (i.e., initiating party) is busy during the recall, the automatic recall will camp on the line. As soon as the originator is free again, the automatic recall is signaled. Either the caller's phone number or that of the destination can be shown on the display or the originator. If the recalled party does not answer the call before the "Intercept time for automatic recall" timer expires, an intercept to the intercept position occurs (if the "On unanswered recall" flag is set). If the intercept position does not answer the recall before the "Time for activation of automatic recall at attendant console" timer expires, the recall is automatically disconnected.

Automatic Recall and Call Pickup

Every station in a call pickup group with the initiating party (originator) can pick up an automatic recall if the system-wide flag "Call Pickup after Automatic Recall" is set.

Automatic Recall and Do Not Disturb

An automatic recall ignores the Do Not Disturb setting.

System-Specific Information

"Intercept time for automatic recall" timer: 30 seconds by default

"Time for activation of automatic recall at attendant console" timer: 60 seconds by default

14.3.7 Call Supervision

Call Supervision allows authorized subscribers to listen in on a call conducted by any internal subscriber. The microphone of the party listening in is automatically muted. The participants in the supervised call are not advised of the supervision operation by any signal such as a tone or display.

The feature is disabled in the default configuration. It may only be enabled if the country-specific legislation permits this. In individual cases, the current country-specific legislation must always be checked before the feature is activated.

Authorized subscribers need a system phone and the Override class of service.

The subscriber you want to supervise must be actively conducting a call. When you start and end call supervision, you may encounter a lapse of up to two seconds of the conversation. The supervised connection is released as soon as one of the stations in the connection is put on hold, transferred or the call is ended. The supervised connection can only be resumed when the station to be supervised is again engaged in a call.

Dependencies

Topic	Dependency
Cordless phones	You cannot use call supervision at cordless telephones because they do not support automatic microphone muting.
Conferencing	Call Supervision restricts the number of possible conferences. Maximum number of conferences possible in the system = maximum number of simultaneous call supervision stations.
Call Supervision	The call can be overridden only using code *944 + station number (not from a menu).
Call Supervision	To enable the use of features at a station, both the station flag **Call Supervision** and the flag **Override class of service** on must be activated. (Feature cannot be used with CSTA monitoring.)

14.3.7.1 How to Activate or Deactivate Call Supervision for a Station

Prerequisites

You are logged into the WBM with the **Expert** profile.

The Override class of service has been activated for the relevant station.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) Navigate in the menu tree under **Stations** > **Station** > **…** down to the desired station (Index - Station Number - Name).
5) Click on the **Edit Station Flags** tab.

6) Select one of the following options:
   - If you want to grant the authorization for this function to a station, select the **Call Supervision** check box.
   - If you want to revoke the authorization for this function from a station, clear the **Call Supervision** check box.
7) Click on **Apply** followed by **OK**.

14.3.8 Discreet Call (Whisper)

The Discreet Call (Whisper) feature enables a subscriber (e.g., at station C) to monitor a simple existing connection between two other stations (e.g., A and B) and to pass on information to station A that without being heard by station B. This feature is typically used in Contact Centers and Executive/Secretary systems.

The feature must be configured in E Manager.

NOTICE: Although there is no connection between station B and station C, user B may be able to hear the muffled tones of what user C is saying because of feedback on station A.

Destination terminals for the Whisper feature (station A) can only be system telephones with displays. Stations A and C must be in the same node.

In the idle/ready state, station C activates this feature by dialing a code. The telephone features a partially programmed key (only the code is programmed on the key, the station number must be suffix-dialed). A new menu item will be incorporated into the Service menu; the Idle/Call menu remains unchanged.

The option for activating the feature is linked to a user-specific class of service. A second class of service can be used to protect station A from a discreet call (whisper/off hook announcement).

The feature is disabled if this is initiated by the activating station C or by the impact of some other call-related feature.

NOTICE: If neither of the participants in the original call is a TDM station, the switching network is not involved at the time of activation, and changeover is impossible without briefly interrupting the existing connection.

NOTICE: Call transfer and conference functionalities are not available from UC Suite products while Discreet Call is activated.

If the Whisper/Off Hook Announcement feature is active, and station A or station B initiates another call-related feature, the Whisper feature will be deactivated. The table below provides further information on interaction with particular features:

Feature	Station A		Station B		Station C	
	Possible	Action	Possible	Action	Possible	Action
Consultation Hold, Call Hold, Park, Common Hold	Yes	Deactivate Whisper/Off Hook Announcement	Yes	Deactivate Whisper/Off Hook Announcement	no	Negative acknowledgement
Transfer	--	--	--	--	--	--
Conferencing	--	--	--	--	--	--
Call waiting	Yes	--	Yes	--	Yes	--
Accept call waiting	Yes	Deactivate Whisper/Off Hook Announcement	Yes	Deactivate Whisper/Off Hook Announcement	Yes	Negative acknowledgement
Override	no	--	no	--	no	--
DTMF transfer	Yes	--	Yes	--	no	--
FEAT counter	--	--	--	--	--	--
Associated Services	--	--	--	--	--	--
DISA/DISI	--	--	--	--	--	--

14.3.9 Live Call Recording (Voice Recording)

This feature is used to record data from an active voice connection between two stations (one station must be internal, the other may be external), in other words, to record calls. A separate device is required for recording.

Recording can be started/stopped by pressing a function key or entering a code (analog telephones). Depending on the configuration, recording can also be stopped by the recording device.

The recording equipment can be used by all supported telephones within a CorNet-NQ network. Connections with CorNet-N and QSIG (ECMA, ISO) are not supported. The recording tone can be deactivated during recording.

TDM and CorNet-IP (HFA) telephones (incl. devices without a display) as well as OpenScape Personal Edition (HFA) and optiClient Attendant are supported. Standard H.323 telephones, SIP telephones and EDSS1 stations are not supported.

NOTICE: Activated voice recording is indicated by a LED or a recording tone during the call.

Authorization to use voice recording can be individually set for each station .

Dependencies/Restrictions

Subject	Dependency/Restriction
Consultation hold, toggle/connect, transfer, conference	Initiating one of these features when recording a call automatically interrupts voice recording.
Call Hold	Ongoing recording is interrupted by activating "Call Hold". Recording cannot be activated when a station is on hold.
Override	Voice recording is not possible. You cannot override a call that is being recorded. Similarly, you cannot activate recording after overriding a call.
Call supervision	Voice recording is not possible. You cannot monitor a call that is being recorded. Similarly, you cannot initiate recording after activating "Call supervision".

NOTICE: You can only record two-party calls, not conferences or calls involving a held party.

NOTICE: Additional remarks:

-) The recording device can be addressed in a random node in a CorNet NQ network.

-) Only a limited number of stations in a node can be allocated voice recording authorization (currently limited to 50 stations).

-) Conference resources are allocated during recording.

-) The default service code for activating call recording is *493.

14.4 Controlling Availability

To control accessibility, the system offers features such as call forwarding, do not disturb and call rejection.

Call destination lists are used for various call forwarding types. Call destination lists define how incoming calls for the assigned station or assigned group are handled. The individual call destinations in a call destination list are processed sequentially. Different entries are possible for internal and external calls (day or night).

14.4.1 Call Forwarding

Call Forwarding—No Answer (CFNA) forwards calls that are not answered within a certain period of time.

This type of forwarding is also referred to as fixed call forwarding, since it is only configurable by the administrator.

For each call forwarding, there are one or more call destination lists, which can be assigned to the stations for the following types of calls:

- External calls during the day (when the night service is inactive)
- External calls at night (during active night service)
- Internal calls

For each call destination list, you can specify up to 4 call destinations to which the call is to be forwarded sequentially after a preset time has expired.

Under normal circumstances, the station number or name of the originally called subscriber and the station number or name of the caller are displayed at the call forwarding destination. As an administrator, you can disable the additional display of the station number or name of the caller.

Call Forwarding on Busy

Call forwarding on busy forwards an incoming call for a busy extension immediately to the next call destination.

If the call destination is also busy, the caller hears a busy signal. For an internal call, the call remains at the call destination, which is cyclically checked until the destination is free. The administrator defines the cycle.

If the call destination is not available and if no further call forwarding has been configured for it, then the call not forwarded.

Dependencies

Topic	Dependency
Analog telephones	There is no indication at these telephones that this call has been forwarded.
Call waiting	If a subscriber enabled call waiting, an incoming call is camped on if call forwarding—busy is configured for him or her.
DND	A call destination which has activated DND, will be skipped.
Call forwarding	Call Forwarding - No Answer (CFNA) is only executed when the call forwarding destination has not responded after a timeout period defined by the administrator.
Night service	If the option "by day / by night" is enabled for a subscriber as the Call Forwarding - No Answer (CFNA) setting, external calls are forwarded in accordance with the settings for the night service. Internal calls are still handled as in the "by day" settings.

Topic	Dependency
External Call Forwarding - No Answer	If external call forwarding - no answer is active, this has precedence over other call forwarding instructions.
Hunt group / Group call	If you enter a group or hunt group as the destination of a call forwarding—no answer instruction, every subscriber in the entire group is called before the next call forwarding destination is evaluated. Group calls and hunt groups can be seen as a call forwarding configuration within a call forwarding configuration. A hunt group is busy if all members are busy or have left the hunt group. A group is always busy if all members of the group are busy.

14.4.1.1 How to Configure Call Forwarding

Call forwarding for internal subscribers can be configured for incoming calls by using the **Call Forwarding** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Call Forwarding** wizard. The **Call dest. list - Definition** window appears.
4) First, define a call destination list by clicking on the **Edit** icon in the row of the call destination list to be processed.
5) Select the desired destinations in the **Target 1** to **Target 4** drop-down lists. You have the following options:
   - **No entry**: The destination is skipped
   - **External destination**: Route and external phone number with CO access code
   - *** Called station**: The called subscriber
   - **** User defined**: Destination of call forwarding after timeout (if configured).
   - **#9 = System search**: Next available station (except for Executive extensions)
   - **#201 - #260**: Call Distribution (UCD Group)
   - **#801 - #817**: Ann. device
   - **100, 101, ...**: Phone number of an internal subscriber or a group (e.g., voicemail box)

NOTICE: To find a call destination faster, you can also enter one or more digits in the **Target 1 - Target 4** fields. This takes you directly to the list item that starts with the

specified string of digits. It is also possible to enter a character string.

---

6) Select the time in seconds after which a call is be forwarded to the next destination from the **Call forwarding starts after:** drop-down list.
7) Select the **Call Forwarding** check box if the call is to be forwarded immediately to the next call destination "on busy".
8) If the call is to be signaled at an additional internal station or at a relay (actuator) for a common ringer (night bell), select the desired phone number from the **Second ringer** drop-down list. With **Sec. ringer type**, select whether the call is signaled at the station immediately or after the entire call forwarding time has expired.
9) Click **OK & Next**. This will return you to the **Basic Configuration** window.
10) If you want to define additional call destination lists, repeat the previous steps.
11) Click **OK & Next**.
12) Now assign the call destination lists to the stations.
13) You can search for a station by typing a search term in the **Call no** or **Name** search fields and then pressing the return key. All matches that contain the search term are displayed. For example, entering the call number `521` would display the matches `+495213535` and `+498967521`, and entering the term `co` as the name would display `Collins`, `Mcoin` and `Branco`.

    NOTICE: Pressing the return key with nothing entered in any of the search fields causes all entries to be displayed.

    ---

14) Select the call destination lists from the drop-down lists in the row of the desired station for the following cases:
    - **Day**: call destination list to be used for incoming external calls during business hours (day service)
    - **Night**: call destination list to be used for incoming external calls during night service
    - **Internal**: call destination list for incoming internal calls
15) Save your entries with **Save** before switching to a station on another page.
16) If you want to assign multiple stations conveniently to a call destination list, click **Copy**.
    a) Under **Call dest. list**, select the call destination to which the stations should be assigned.
    b) Mark one or more stations in the **Selection** window and transfer them with **Add** to the **Members** window.
    c) Use the **Day**, **Night** and **Internal** check boxes to select whether the call destination list is to apply to incoming external calls during working hours (day service), when the night service is activated or only to internal calls.
    d) Click **OK & Next**.
17) Click on **OK & Next** again.
18) You can have all stations of a call destination list displayed here. To do this, select the desired call destination list in **Show all members with call destination list**.

19) Click **OK & Next**. The setup of call forwarding for internal stations is now complete.
20) Click **Finish**.

14.4.2 Call Forwarding (CF)

Subscribers can use Call Forwarding (CF) to redirect incoming calls to a destination of their choice.

If trunk keys (incl. MULAP trunk keys) have been configured, users can also activate call forwarding individually for a specific trunk (or MULAP trunk).

The following calls can be diverted:

- All calls
- External calls only
- Internal calls only

The following destinations are possible for call forwarding:

- Other phone (internal or external)
- Attendant Console
- Voicemail
- Hunt Group
- UCD group (UCD Universal Call Distribution)

Outgoing calls can still be made when call forwarding is activated.

External destination

If the call forwarding destination is external, you must enter the trunk access code followed by the external phone number of the forwarding destination.

Call Forwarding to External Destinations

If a subscriber has entered an external call forwarding destination in his or her call destination list, forwarding ends at this destination, and any further call forwarding destinations that may have been entered in call destinations list are ignored.

If call forwarding to additional destinations is to occur, the system flag **Hunting to external call forwarding destination** must be activated by the service technician.

If call forwarding to an external destination is to be followed even for a call over an analog trunk, the system flag **Call forwarding to main station interface permitted** must be activated by the service technician.

NOTICE: When a call is routed through Smart AA and this call is put through towards a user A with external forward activated (*11) to user B, then user B will not be presented the calling party CLI, but user A's DID.

Dependencies

Topic	Dependency
Do Not Disturb	You cannot program call forwarding to a telephone where DND is active.
Appointment, automatic wake-up system	If an appointment comes due, it is signaled at the forwarded telephone, irrespective of any active call forwarding settings.
UCD group as call forwarding destination	A call is not forwarded to a UCD group in the following cases: • If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called. • A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group. • A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.

14.4.2.1 How to Enable or Disable Call Forwarding over Analog Trunks

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **System Flags**.
4) Select one of the following options:
   - If you want to enable call forwarding over analog trunks, select the **Call forwarding to main station interface permitted** check box.
   - If you want to disable call forwarding over analog trunks, clear the **Call forwarding to main station interface permitted** check box.
5) Click on **Apply** followed by **OK**.

14.4.2.2 How to Enable or Disable Call Forwarding to the External Destination

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.

3) Navigate in the menu tree to **System** > **System Flags**.
4) Select one of the following options:
   - If you want to enable call forwarding to the external destination, select the check box **Hunting to external call forwarding destination**.
   - If you want to disable call forwarding to the external destination, clear the check box **Hunting to external call forwarding destination**.
5) Click on **Apply** followed by **OK**.

14.4.3 Call Forwarding After Timeout

Call Forwarding after Timeout forwards unanswered calls after a specific period of time. Call Forwarding after Timeout is analogous to Call Forwarding No Answer, the only difference being that subscribers can set the call forwarding themselves.

The subscriber can set call forwarding after timeout for his or her own phone and can also enter external destinations and groups.

The call deflection destination is not permanently saved, but deleted after you deactivate the feature.

If a subscriber is busy, the rules of call forwarding - no answer apply, that is, the system proceeds to the next destination.

System-Specific Information

You can set three destinations for each station. In addition, there is also a special ID "User-defined", via which the administrator can release or lock the Call Forwarding after Timeout feature for a station. The feature is released by default.

If a call is not answered after the preset timeout, the system searches for and calls the call deflection destination saved. If the subscriber has not entered an individual call deflection destination, the system proceeds with the next destination in the call destination list.

The administrator must release the call forwarding after a timeout for the individual subscribers via the call destination lists.

14.4.4 External Call Forwarding - No Answer (Not for U.S.)

Every station assigned an MSN (multiple subscriber number at the ISDN point-to-multipoint connection or ITSP connection) as a DID number can activate or deactivate call forwarding —no answer for this MSN, provided that the user is authorized to use external call forwarding—no answer.

If you have assigned an MSN to a subscriber group, any member of the group can activate and deactivate external call forwarding-no answer for this MSN.

There are three different versions of the feature:

- Call Forwarding Unconditional (CFU): The network provider forwards all calls to this MSN directly, regardless of the MSN status.
- Call Forwarding Busy (CFB): Calls are forwarded only if the MSN dialed is busy.

- Call Forwarding No Reply (CFNR): Calls are forwarded only if the destination does not answer the incoming call within a preset period of time.

NOTICE: For all the above call forwarding scenarios, users can enter only one forwarding destination per MSN. A total of 10 multiple subscriber numbers can be forwarded.

In case of ITSP or ISDN configured with DID, this number is 249.

Dependencies

Topic	Dependency
Night service	External call forwarding—no answer has a higher priority than night service.

14.4.5 Ringing Assignment / Call Allocation

The ringing assignment enables incoming calls of an analog or S_0 trunk to be forwarded to a station or group, depending on the dialed number and the activation state of the night service.

Different destinations are possible for the day and night service. An incoming call is not signaled at the called station, but according to the call destination lists for that station.

14.4.5.1 How to How to Configure a Ringing Assignment

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) Click on **Trunks/Routing** > **Trunks** in the menu tree.
4) Navigate in the menu tree under **Trunks** > **…** (Box-Port code) to the desired analog or S_0 trunk.
5) Select the desired station number in the **Day Call no.** drop-down list.
6) Select the desired station number in the **Night Call no.** drop-down list.
7) Click on **Apply** followed by **OK**.

14.4.6 Ringing group on

The feature "Ringing group on" allows internal subscribers to manage a personal list of internal call numbers which are called whenever their own number is called.

Users can also enter their own station numbers. They might do this, for example, if a station number is permanently routed to another station (executive/secretary).

A button can be programmed on the IP system telephones, OpenStage TDM telephones and optiPoint 500 telephones to activate/deactivate this feature. More than one Ringing Group button can be programmed on one telephone to allow for different variations. More than one button can be activated at one time; however, the maximum number of telephones with call signaling cannot exceed five.

This feature can be activated/deactivated via a DISA connection by its own station user or for another user with the aid of the feature Associated Services.

The Forwarding screen is one of three screens in the System Status pathway in Manager E that provides station-specific (rather than system-specific) status information. You can use the Call Forwarding screen to see if a phone has a Ring Group activated or if it is part of a Ring Group.

If the feature is used frequently, the subscribed can assign the feature to a free button on the telephone. The name of the key is "Ringing group on" under Key Programming. When the feature is enabled, the LED is lit.

The station flag “no group ringing on busy” determines which stations in a call ringing group receive a call when the master telephone (the one activating the feature) is busy, and which ones do not. If the same station is in the ringing group of more than one master telephone, the flag applies to all calls signaled at this station.

If the flag is not set, group ringing always takes place, provided the station in the call ringing group is available (default behavior).

If the flag is set, group ringing depends on the availability of the master telephone:

- If the master telephone is available, group ringing takes place immediately

  If the primary telephone has activated call waiting, group ringing takes place after a 5-second delay.

  If the primary telephone cannot receive a call, or if call waiting is inactive, call ringing does not take place.

Topic	Dependency/Restriction
Automatic recall System search Callback	Group ringing is not carried out with an immediate recall (operator error), system search or callback.
Call forwarding	If the station that activated group ringing has also activated call forwarding, group ringing does not occur.
Do Not Disturb (DND)	If a station in the call ringing group has activated DND, group ringing is not carried out at that station.
Timed reminder	An active timed reminder does not follow group ringing.
No group ringing on busy	If the flag is set, no group ringing will take place if the station is busy.

14.4.7 Rejecting Calls

The subscriber can reject internal and external incoming initial calls. These calls can be rejected by pressing the Disconnect key.

The rejected call is then forwarded in accordance with the CFNA instruction. If there is no other call forwarding destination, an external call is intercepted by the attendant console, provided the relevant intercept criteria were configured. If no destination can be called, the caller continues to receive a busy signal.

Transferred recalls, transfered calls, queued callbacks, held or parked calls cannot be rejected. An intercepted call sent to the Intercept position cannot be rejected.

Dependencies

Topic	Dependency
Group call, hunt group call, MULAP	In these cases, the entire group call is terminated and the call follows the call forwarding instruction configured. The call is terminated if there is no other call destination.

14.4.8 Deferring a Call

Subscribers are provided the option of deferring an incoming call. The subscriber called can set up a connection without picking up the incoming call.

The waiting call is then signaled as a camped-on call.

If an incoming call is signaled, the subscriber can press a call or trunk key to conduct the external call. Two call keys and one trunk key must be programmed for this. One of the relevant keys must be free to execute the feature.

The calling party does not notice a change in signaling if call waiting is set for ringing on call waiting.

14.4.9 Do Not Disturb

Do Not Disturb prevents incoming calls from being put through.

A subscriber who has activated DND hears a special dial tone when he or she lifts the handset. When active, the Do Not Disturb feature is also indicated on display phones. In all other phones, the LED on the DSS key flashes with a brief interruption on stations where Do Not Disturb is active.

The Do Not Disturb feature, if set, can be overridden by the Attendant or an authorized subscriber. The call can also be immediately put through for a subscriber with an active Do Not Disturb feature.

A caller who dials a telephone with DND activated receives a busy signal and is not allowed to camp on.

Dependencies

Topic	Dependency
Attendant/night destination	The attendant and the current intercept position cannot activate the Do Not Disturb feature.
Call forwarding	You cannot specify DND if call forwarding is active on the same telephone. You cannot activate call forwarding to a telephone with DND.
Callback	If a callback is initiated to a station with DND activated, the callback is not executed until DND is deactivated. If the subscriber with DND activated initiates a callback, this will override the DND function.
Appointment, automatic wake-up system	If a station has set an appointment and activated DND, an audible signal is sent to the telephone when the appointment comes due.
DISA	DISA can be activated by the subscriber for his or her own phone or by a user for another phone (associated services).

14.5 Optimizing Communication

The communication system offers various options to conveniently and effectively handle calls, e.g., through callbacks or call waiting.

14.5.1 Callback

A callback can then be activated if the subscriber called does not answer or is busy. An active callback triggers a call as soon as the called subscriber is available.

Automatic Callback When Free or Busy

If a call cannot be set up because the subscriber called is busy or does not accept the call, the calling subscriber can activate a callback to set up the call at a later time. If the subscriber called was busy, the Callback function monitors the call to see when it ends. The calling subscriber receives a signal in the form of a call from the communication system when the other subscriber's line is free. If he or she accepts this call, the subscriber who was previously busy is redialed. If a call set up via the Callback function is not successful, this function remains active. The callback attempt is repeated once the required subscriber has conducted another call.

A telephone can initiate up to two Callback requests and be the destination for up to two requests. Any further outgoing requests are rejected.

Callback requests are deleted when

- the call is completed; if not, the callback remains in effect (for an internal callback),
- the callback was established without a call being completed (for an external callback),

- the initiator cancels the request,
- the system deletes all callbacks daily at 23:57.

Callback requests can be made for internal subscribers and groups. Callback requests for a group call are stored at the first subscriber. When a callback is made to a group, the ring is heard at all phones that are free.

Automatic Call Completion on No Reply (CCNR) on the Trunk Interface

An internal subscriber who cannot reach an available external subscriber can activate a callback request at the central office. The system then monitors the connection of the called subscriber. As soon as the called subscriber initiates a connection setup and then ends this connection, the central office attempts to establish a connection between the two subscribers. This feature must be supported by the central office.

Callback on busy

This feature sets enables a manual callback to be set on an external station that is busy. When the station becomes free, the trunk attempts to set up a connection between the two stations. The feature must be supported and enabled by the central office and peer.

14.5.2 Call Waiting

Call waiting signals the arrival of a further incoming call to a subscriber who is on the phone.

The incoming call is visually signaled by a message on the display. It can also be signaled acoustically by a short call waiting tone. The call waiting tone can be heard every 5 seconds.

The subscriber called can accept this second call or ignore it. To answer the second caller, the subscriber can optionally end the first call and answer the second or select the **Call waiting** function offered in the display. In the latter case, the first call is placed on hold.

You cannot camp on to a subscriber if someone is already camped on (a maximum of 4 subscribers can camp on) or if the subscriber has activated call waiting rejection. The caller receives a busy signal if call forwarding—busy is not configured.

Enabling Call Waiting

Call Waiting (Camp On) by Attendant Console

If the **Call waiting rejection** flag is set, the subscriber can use a menu or code to either enable or suppress call waiting. If a subscriber has enabled call waiting, an incoming call is camped on if call forwarding—busy is configured.

The default setting is always "call waiting after timeout". However, the Attendant Console can also camp on immediately.

Dependencies

Topic	Dependency
Call waiting tone	The subscriber can activate/deactivate the call waiting tone with a code. Call waiting is still visually signaled on the phone's display. The call waiting tone is active by default.
Override	If call waiting rejection is active, an ongoing call by this subscriber cannot be overridden.
Group Call	If one or more stations in a group call are free, the call will be offered to them. If all stations are busy, all of them receive a call waiting signal, apart from any stations where call waiting rejection is active.
Speaker call	Speaker calls to busy stations are not possible.

14.5.2.1 How to Enable or Disable Call Waiting

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) Click **IP Clients**, for example.
5) Click **System Clients**, for example.
6) Select the relevant station.
7) Click on the **Edit Station Flags** tab.
8) Select one of the following options:
   - If you want to enable call waiting, clear the Call waiting rejection on check box.
   - If you want to disable call waiting, select the check box **Call waiting rejection on**.
9) Click on **Apply** followed by **OK**.

14.5.2.2 How to Enable or Disable Immediate Call Waiting (Camp On) by the Attendant Console

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.

4) Click on **Intercept/Attendant/Hotline**.
5) Select one of the following options under **Other criteria**:
   - If you want to activate the function, enable the check box **Immediately camp on for attendant calls**.
   - If you want to deactivate the function, clear the check box **Immediately camp on for attendant calls**.
6) Click on **Apply** followed by **OK**.

NOTICE:

For CMI DECT - TDM deskphones, when a station that is busy is called and call waiting - camp on is allowed, the busy tone is active for 5 seconds, and then camp on takes place thus the ringback tone can be heard.

For IP DECT - SIP deskphones when a station that is busy is called and call waiting - camp on is allowed, the camp on is immediate thus the ringback tone can be heard from the beginning.

14.5.3 Override (Intrusion)

The Override feature enables an authorized subscriber to override (i.e., intrude into) a call of another internal subscriber.

The override (intrusion) occurs by means of a code or key, and the subscriber involved is notified by a warning tone (beep) and a visual signal on the display.

The feature can be invoked during the busy signal or during the camp on state.

During an override condition, the following applies:

- If the called party hangs up, he or she receives a call from the switching party.
- If the overriding party (who wants to switch the call and overrides) hangs up, the call is switched through to the destination station.
- If the party which was connected to the called party hangs up, the overridden and called parties remain connected.

An override can be performed by any internal subscriber and the intercept position (attendant console). However, in order to use this feature, the internal subscriber and even the intercept position must be authorized for this.

It is not possible to prevent an override to a particular telephone.

Dependencies

Topic	Dependency
Voice Channel Signaling Security	You cannot override a call if the called station or the internal party it is connected to is entered as a data station (voice channel signaling security), or if the called party is dialing a number.
Do Not Disturb	If the called station has activated Do Not Disturb, only one call can be overridden when the subscriber is conducting a call.

Topic	Dependency
Hunt group	Busy override is not possible if all stations are busy when a group or hunt group is called.
S_0 station	It is not possible to override an S_0 station.

14.5.3.1 How to Authorize an Internal Station for the Override Feature

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) In the menu tree, click the station (Index - Call number - Name).
5) Click on the **Edit Station Flags** tab.
6) Activate the check box **Override class of service on**.
7) Click on **Apply**, followed by **OK**.

14.5.3.2 How to Authorize the Intercept Position for the Override Feature

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click on **System** > **Intercept/Attendant/Hotline** in the menu tree.
4) Select the **Override by Attendant** check box in the **Other criteria** area.
5) Click on **Apply** followed by **OK**.

14.5.4 Advisory Messages

The advisory message of a subscriber appears in the caller's display.

Variable parameters can also be assigned in advisory messages (also referred to as absence texts). These parameters (for example, time) are entered in the course of activation. Users can use the numeric keypad on the telephone to enter additional characters. The advisory message can be activated/deactivated at a phone via a code or a preconfigured function key.

Call forwarding

When call forwarding is enabled, the called subscriber's advisory message is displayed and the call is forwarded.

14.5.4.1 How to Edit Advisory Messages

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **Texts**.
5) Click on the relevant field in the **Answer texts** column and enter your advisory message.
6) Click on **Apply** followed by **OK**.

14.5.5 Message Texts

Message texts are internal system texts that can be selected by a subscriber and sent to internal subscribers.

A message text (also called an Info text) can be sent to one or more recipients.

If you want to send the text to all members of an internal group or an internal hunt group, you must specify the phone number of the group or the hunt group - not an individual subscriber - as the recipient.

NOTICE: Only 100 phones can receive mass Message Waiting Indication (MWI) messages, any additional message will fail.

The message is sent by pressing the relevant button or via the Send Message menu.

The message can be sent in idle, ringing, talk or busy state. In ringing state it is not necessary to specify the recipient's station number.

14.5.5.1 How to Change a Message Text

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **Texts**.
5) Click on the relevant field in the **Info texts** column and enter the text.
6) Click on **Apply** followed by **OK**.

14.5.6 Associated Services

An authorized station can control certain features on behalf of any other station, e.g., call forwarding, turning the lock code or hunt group on/off, etc. The effect is the same as if the feature involved were activated or deactivated by the other station itself.

The following features can be controlled on behalf of other stations:

- Call forwarding on / off
- COS changeover on / off
- Ringing group on / off
- Advisory message on / off
- Hunt Group and Group Call on / off
- Night service on / off
- Timed reminder on / off
- Send message / Delete sent message
- Edit lock code password
- UCD agent log in / log out
- UCD agent Available/Not available
- UCD agent Wrapup on / off
- UCD agent Night service on / off
- Forward Line Key (MULAP) on / off
- Resetting Activated Features

This is operated via a procedure. The station must specify the following:

- the code for Associated Services
- the station number of the subscriber for whom the action is to be performed.
- the code of the feature to be controlled

Before any subscriber can use the Associated Services, he or she must first disable the lock code of the other subscriber (if enabled).

14.5.6.1 How to Activate or Deactivate Associated Services

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click on **Telephony** > **Stations**.

3) In the menu tree, click **Stations**.

4) In the menu tree, click the station (Index - Call number - Name).

5) Click on the **Edit Station Flags** tab.

6) Select one of the following options:

- If you want to activate the function, select the check box **Associated dialing/services**.
- If you want to deactivate the function, clear the check box **Associated dialing/services**.

7) Click on **Apply** followed by **OK**.

14.5.7 DISA

DISA (Direct Inward System Access) allows authorized subscribers to use features of the communication system from outside, e.g., at the mobile phone using myPortal for Mobile (for mobile callback) and Mobility.

Using DISA, a subscriber can also set up outgoing connections, both internal and external. Whenever a subscriber uses DISA, he or she must enter the password for the lock code. Certain features are then available as for internal use.

DISA supports the following features:

Feature	by the subscriber him/herself	via associated services
Call forwarding on / off	x	x
Do not disturb on / off	x	x
Hunt group on / off	x	x
Advisory message on/off	x	x
Ringing group on / off	x	x
COS changeover on / off	x	x
Reset services	x	x
System Speed Dialing	x	–
Send message text	x	–
Night service on / off	x	–

The administrator specifies under which call number the stations can access DISA. The call number may be different for external and internal use. Internal means at some other "IP-networked" node.

The password to be entered by subscribers consists of the internal call number and the PIN for the lock code. After entering the password, subscribers must either press the # key or wait until the communication system has recognized their input, depending on the security mode that was set for DISA by the administrator.

The subscriber must log in again for further action via DISA.

NOTICE: In OpenScape Business X when a DISA number is called, you will hear a coninuous tone. In OpenScape Business S when a DISA number is called, you will hear Music on Hold.

14.5.7.1 How to Activate or Deactivate a DISA Class of Service for a Station

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) In the menu tree, click the station (Index - Call number - Name).
5) Click on the **Edit Station Flags** tab.
6) Select one of the following options:
   - If you want to activate the function, select the check box **DISA Class of Service**.
   - If you want to deactivate the function, clear the check box **DISA Class of Service**.
7) Click on **Apply** followed by **OK**.

14.5.7.2 How to Configure a DISA Number

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **DISA**.
4) In the field **DID**, enter the call number via which the stations can use DISA externally.
5) In the field **Phone Number**, enter the call number via which the stations can use DISA internally.
6) Click on **Apply** followed by **OK**.

14.5.7.3 How to Configure the DISA Security Mode

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **DISA**.
4) In the **Security Mode** drop-down list, select the item **After timeout** or **After input #**.
5) Click on **Apply**, followed by **OK**.

14.5.8 Flex Call/Mobile PIN

Flex Call (Mobile PIN) enables a system telephone to be temporarily used by other subscribers for the next outbound call as if that phone were their own phones.

Flex Call includes this subscriber's phone number, name, toll restriction, and call detail recording.

The phone being used cannot be reached at its own station number if Flex call is enabled. This status is reverted at the end of the call.

To enable Flex Call, an individual code lock must have been assigned for the mobile subscriber.

One of the following steps must be performed at the system phone to activate the feature:

- OpenStage: Service Menu > PIN and Class of Service > Flex Call + Mobile phone number + Lock code of mobile subscriber
- Code for Flex Call + Mobile phone number + Lock code of mobile subscriber

14.5.9 Relocate

The Relocate (Hoteling) feature allows an OpenStage TDM station to use a procedure to change the assignment between the physical telephone port and the logical station data (user profile).

The Relocate feature can be used if two users decide to swap their workplaces and both users share the same phone types. Relocate thus enables the implementation of DeskSharing for TDM users. The TDM users can perform the Relocate operation without the assistance of an administrator.

Only user profiles of the same phone type, i.e., with an identical key layout, may be exchanged. If you exchange user profiles from different phone types, individually programmed key functions on the basic device will be replaced by the default values. Executing the Relocate feature causes the TDM telephones involved to go out of service and restart. Enabled features are treated accordingly, i.e., current callbacks and sent infos are deleted, and all other features are preserved.

The use of Relocate requires a system-wide release of the feature. To enable the feature, select Relocate in the service menu of the phone to be exchanged and enter the internal number of the target station and the lock code PIN (the lock code PIN is not required if the default PIN 00000 is being used). After you have entered the destination call number, the Relocate feature is blocked for all other users until the procedure has completed. When executing the exchange, both telephones involved are reset. The successful exchange is indicated on both TDM phones by the display of the new number (display: New Call No.: XXXXX).

Relocate cannot be performed on system telephones with programming authorization (for Assistant T). In other words, Relocate is usually not possible on the first two active system telephones.

14.5.9.1 How to Unlock Relocate on a System-wide Basis

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Basic Settings** > **System**.
3) Click **System Flags** in the menu tree.
4) Select the **Relocate allowed** check box.
5) Click on **Apply** followed by **OK**.

14.5.10 Reset activated features

You can reset specific features collectively at your terminal using a code.

This is possible for the following features:

- Call forwarding
- Delete received infos
- Advisory message on / off
- Ringing group on / off
- Hunt group on / off
- Station number suppression on / off
- Silent camp-on on / off
- Do not disturb on / off
- Ringer cutoff on / off
- Appointment
- Cancel all callbacks

14.5.11 Procedures

The communication system lets the subscriber program a key with codes, phone numbers, and other dialing information. If a subscriber presses the Procedure key as a suffix or during a call, the communication system transmits the corresponding DTMF character (DTMF = dual tone multifrequency).

Sample applications:

- Code for callback
- Code for call waiting
- Code for override
- Digit string for voicemail or answering machine
- Trunk flash code + destination station number
- Code for controlling a service + destination phone number, for example, code for send/retrieve message (message waiting) + phone number + text number
- ACCT (account code) + trunk code + destination station number

Procedures that require PIN input cannot be saved.

Only the first key level supports Procedure keys.

Depending on the situation, a subscriber can use the following features in procedures:

Feature	Ready to dial	Busy	On the phone	Outgoing call	Incoming call
Directed call pickup	x	–	x	–	–
Call Forward on, (not for tenant systems; not for individual MSNs in an S_0 trunk connection)	x	–	x	x	–
External call forwarding on / off; toggle function; (not for tenant services);	x	–	x	x	–
Call forwarding, login/UCD (uniform call distribution), logout; toggle function	x	–	x	x	–
Call forwarding, night destination on / off; toggle function	x	–	x	x	–
Call forwarding per team configuration	x	x	x	x	x
Advisory message on / off; toggle function	x	–	x	x	–
Associated Dialing	x	x	x	x	x
Associated Services	x	–	x	x	–
Speaker call	x	–	x	–	–
Release trunk (emergency trunk access)	x	–	x	x	–
Send message (message waiting)	x	–	x	x	–
Dial station speed dialing	x	–	x	x	–
Dial system speed dialing	x	–	x	x	–
DTMF transmission	–	–	x	–	–
DTMF transmission in the talk state using procedure key	x	x	x	x	x
Night service on / off; toggle function	x	–	x	x	–
Retrieve call; toggle function	–	x	x	x	–
Account code ACCT	x	–	x	–	–
Account code ACCT in prefix	x	–	x	–	–
Callback requests - display or delete; toggle function	x	–	–	–	–
Ringing group on / off; toggle function	x	–	x	x	–
Language selection	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Door opener via adapter cabinet	x	x	x	x	x
Timed reminder; toggle function	x	x	x	x	x
Retrieval of an external call from common hold	x	x	x	x	x
System Telephone Lock	x	–	x	–	–

System-Specific Information

A procedure key can store up to 32 characters.

14.5.12 Automatic Wake-up System and Timed Reminders

All users can program timed reminders (appointments). They will be reminded of the appointment at the set time. The appointment can be programmed for a single reminder (once within a 24-hour period) or for regularly scheduled daily reminders.

The time format is four-digits. The first two digits are the hour, and the second two digits are the minutes. A 12-hour clock mode is supported for the U.S.: users enter the four digits and then select "am" (key 2) or "pm" (key 7). If nothing is specified, "am" will be used as the default setting.

Analog telephones, optiPoint 500 and CMI telephones support only programming of non-repeating appointments.

The default timed reminder sounds for 20 seconds and will repeat a maximum of five repeats at one-minute intervals. The timed reminder is cleared automatically as soon as the user lifts the handset or presses the speaker button, or after the fifth repeat (number of repeats is configurable). Alternatively, a programmed timed reminder can be canceled using a procedure. Display telephones also support queries.

A timed reminder which is due but cannot be signaled (user busy, for example), is postponed until the next cycle.

INFO: Timed reminders can be scheduled for up to 50 users, per system.

14.6 Overview of functions and codes

Service code	Description
*0	Return to held call
*1	Call forwarding
*2	Toggle/Connect
*3	Conference
*44	Night answer on
*51	Trunk flash
*52	Mute on
*53	DTMF dialing
*55	Accept call waiting
*56	Park call
*57	Call Pickup (Group)
*58	Initiate callback
*59	Directed Call Pickup
*60	Account code
*61	Door opener

Service code	Description
*62	Override
*64	Call forwarding to CO (ISDN)
*65	View call charges
*66	COS changeover on
*67	Associated dial
*68	Send message
*69	Advisory message on
*7	Use speed dialing individual/system
*80	Speaker call
*90	Relay on
*91	Key programming
*92	Change individual speed-dial numbers
*93	Change PIN
*940	Phone test
*95	System Administration
*97	Do Not Disturb on
	Room Monitor
*81	Ringing group
#1	Call forwarding off
#44	Night answer off
#52	Mute off
#56	Retrieve call
#58	View/delete callback(s)
#64	Cancel call forwarding to CO (ISDN)
#66	Changeover off
#68	View sent message
#69	Advisory msg. off
#97	Do Not Disturb off
*96	Hands free answerback on
#96	Hands free answerback off
#90	Reset relay
#81	Ringing group off - all members removed
#0	Reset all services
#3	Conference off
#82	Query Caller List

Service code	Description
*83	Associated services
*84	MCID
*85	Rejoin hunt group
#85	Leave hunt group
*82	Missed calls - save number
*86	Suppress calling ID
#86	Enable calling ID
*87	Waiting tone off (external)
#87	Waiting tone on (external)
*98	Ringer cutoff on
#98	Ringer cutoff off
*991	Start DTMF remote administration
*992	Allow DTMF remote administration
*993	Allow ISDN remote administration (obsolete)
*994	Allow remote data query (inactive)
*89	Release door opener with DTMF code
#89	Lock door opener with DTMF code
*63	Continue an external call after the hold key
*41	Assign station numbers (MUSAP)
*401	Log on UCD agents
#401	UCD - agent log off
*402	UCD - agent available
#402	UCD - agent not available
*403	UCD work on
#403	UCD work off
*404	UCD night service on
#404	UCD night service off
*405	UCD - calls in queue
*42	Telephone Data Service (TDS)
*43	Release trunk
*45	PSE: locate
#45	PSE: answer
*46	Timed reminder on
#46	Timed reminder off

Service code	Description
*9419	Activate relocate
#9419	Deactivate relocate
*942	Ready for login (CMI phone)
*943	System telephone lock
*944	Call supervision
	Drop Last Conference Party within CO (USA only)
*490	Call waiting terminating on
#490	Call waiting terminating off
*48	Language selection
*508	Flex Call
*502	Ring transfer for MULAP on
#502	Ring transfer for MULAP off
*501	Call forwarding for MULAP on
#501	Call forwarding for MULAP off
*509	Freeze trace
*47	DISA internal
*503	Keypad dial
*54	Internal Phonebook
*491	Analog Hoteldevice
#943	Reset central codelock
*9411	Call Forwarding Client in Emergency mode on
#9411	Call Forwarding Client in Emergency mode off
*493	Voice recording on
#493	Voice recording off
*495	Call forwarding after time on
#495	Call forwarding after time off
*945	Discreet Call
*494	Data I/O
*996	Allow Smart Services via HTTPS for remote administration
#996	Disable Smart Services via HTTPS for remote administration
*997	Controlled shutdown

15 Working in a Team (Groups)

Several features are provided by the communication system to enable and facilitate working in a team. Besides call pickup groups, group calls and hunt groups, this also includes groups with team and executive/secretary functions as well as voicemail box and fax box groups. The "UCD (Uniform Call Distribution)" feature enables incoming calls to be uniformly distributed to a group of users (UCD group).

INFO: When configuring groups, it must be noted that the first three are reserved:

The first group is used by default as the hunt group for External Voicemail.

The second group is used by default as the hunt group for OpenScape Business Smart VoiceMail.

The third group is used by default as the hunt group for the Company AutoAttendant of OpenScape Business Smart VoiceMail.

15.1 Call Pickup Group, Group Call and Hunt Group

The communication system offers several methods of combining stations into groups so that multiple subscribers and phones can be reached under one call number, for example, or a call to one station can also be signaled at other stations.

In the case of a call pickup group, a call for one member of the group is also signaled at all other group members.

With a group call, by contrast, all members can be reached via a single phone number (group phone number). The first station to answer the call is connected to the calling party.

In the case of a hunt group, an incoming call is signaled at one of the group members. If this member does not answer the call, the call is assigned to the next member. All members of the hunt group can be reached at the same phone number.

15.1.1 Call Pickup Group

A call for a member of a call pickup group is also signaled at all other group members. The call can be accepted by all group members via a function key programmed for this purpose, via the associated phone menu item or by dialing the code.

The call is signaled acoustically and visually on the display of the call pickup group member originally called. If programmed, the call is also signaled via the function key LED.

The other group members are only notified of the call by a visual signal. The phone number or name of the subscriber originally called and the phone number or name of the caller are shown on the phone's display. The display of

the station number or name of the caller can be disabled by an administrator with the **Expert** profile in **Expert mode**. If programmed, the call is also signaled via the function key LED.

If the call is not accepted within four ring cycles (4 x 5 seconds), the other group members receive a warning tone (acoustic signaling). The time from the start of call signaling till the warning tone is not variable. The warning tone can be disabled for all group members by an administrator with the **Expert** profile in **Expert mode**.

If more than one call is received for a call pickup group, signaling occurs in the sequence in which the calls are received.

If recalls for members of a call pickup group are also to be picked up by other members in the group, this must be enabled by an administrator with **Expert** profile in **Expert mode**.

A station can belong to only one call pickup group.

Any call charges incurred for a picked-up call are accrued to the subscriber who picked up the call.

NOTICE: Double quotations (") are not supported for naming a Call Pickup Group.

SIP Phones

SIP telephones can be integrated in a call pickup group.

INFO: In addition, a function key for the call pickup group can be programmed for SIP phones, and the specific messages of a call pickup group can be shown on the displays of the corresponding SIP phones. In order to use this feature, the "Call Pickup Group" feature must be enabled on the SIP phone (see the User Guide of the SIP phone for details).

Call Pickup Outside a Call Pickup Group

Another version of the feature is the "call pickup outside a call pickup group". This permits the pickup of calls for internal subscribers that do not belong to the same call pickup group. The call can be picked up via a function key programmed for this purpose, the associated menu item or by dialing the specific call pickup code followed by the station number of the called station.

Dependencies

Topic	Dependency
Callback	Recalls and callbacks are signaled at the other group members only if the system flag **Call Pickup after automatic recall** has been activated.
Do Not Disturb	Stations that have activated DND do not receive call pickup signaling.
ISDN Phones	It is not possible to include ISDN telephones in call pickup groups.

Topic	Dependency
MULAP	It is not possible to include MULAP phone numbers in call pickup groups.

Related tasks

How to Configure a Call Pickup Group on page 660
How to Add or Delete a Member to or from a Call Pickup Group on page 660
How to Enable or Disable the Display of a Caller's Station Number and Name on page 668
How to Activate or Deactivate the Warning Tone on page 668
How to Enable or Disable Call Pickup for Recalls on page 668

15.1.2 Group Call

A group call can be defined in cases where multiple subscribers need to be reached via a single phone number (group phone number). Incoming external and internal calls are signaled at the same time at all group member phones. The first station to answer the call is connected to the calling party.

Every member of a group call can also be reached at his or her own station number.

The group must be assigned one of the following properties:

- Group

  Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. If all group members are busy, a call is signaled by a camp-on tone. Call signaling continues at all group members (camp-on tone at busy group members) even if the subscriber hangs up.

  A caller hears the busy tone if all group members are busy and all have activated the DND feature. If a call forwarding destination has been defined for this group, the caller does not hear a busy tone, but is forwarded directly to the next call forwarding destination.
- RNA

  Incoming calls are simultaneously signaled at all group members. If a group member is busy, the entire group call is marked as busy. Other callers receive the busy tone.

  NOTICE: The presence status of an external destination that belongs to the group cannot be detected.
- Call waiting

  Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. A call is signaled by a camp-on tone for busy group members.

  This requires that all group members have the Do Not Disturb feature disabled.

Group calls are treated like stations by the Call forwarding—no answer function. In other words, if a call cannot be accepted by any of the members in a group

call, it is redirected to a call forwarding destination in accordance with the call destination list. You can specify whether call forwarding should be performed on RNA (ring no answer) or busy.

When a call is not answered by any member of a group call, it appears as a missed call in the journal of the UC clients of all members. An accepted call appears only in the journal of the member who answered the call.

A single station can belong to several groups simultaneously. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

The group name assigned is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for group calls.

Up to 20 subscribers can be configured per group call.

Every group call can be assigned a name containing up to 16 characters.

Voicemail Box for Group Call

When setting up a group call, a voicemail box is created automatically. The call number of this voicemail box for the group call always matches that of the group call. If a group call is not accepted by any member, the call is forwarded to the voicemail box for the group call. This requires the group call voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this group call.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

Example of a group call of type RNA (ring no answer) with the group call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the group call was set up for the group call. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.		
Inbound call for Member A (200)	All members are free.	Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is forwarded immediately (CFU) to the voicemail box of member A.

Inbound call for the group call (404)	All members are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is signaled at members B and C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.	The call is signaled at members B and C and at the external destination. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.

Activating/Deactivating a Group Call

If a subscriber is a member of a group call, he or she can use codes to leave and rejoin the group call.

If a subscriber is a member of both multiple group calls and multiple hunt groups, he or she can use codes to leave and rejoin all group calls and hunt groups. Subscribers are added to or removed from a specific group call or hunt group by entering codes and then making a selection from the group calls and hunt groups displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific group call and hunt group or all group calls and hunt groups. Variable programming is also possible. After you press a function key of this kind, you must select one of the group calls and hunt groups displayed to define the group call or hunt group you want to leave/join.

Ring type

For every group call, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in a group call.

NOTICE: No programming of function keys is possible for SIP phones. Specific display messages of a hunt group are not supported.

Dependencies

Topic	Dependency
Call forwarding	If a group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls via the group phone number and the member's own station number.
Override	Override is not possible if all members of a group call are busy.
ISDN Phones	It is not possible to include ISDN telephones in a group call.

Related concepts

Internal Directory on page 489

Related tasks

How to Add a Group Call (Group) on page 661
How to Edit a Group Call (Group) on page 662
How to Delete a Group Call (Group) on page 663
How to Add or Delete a Member to or from a Group Call (Group) on page 664
How to Add a Group Call (RNA or Call Waiting) on page 669
How to Display or Edit a Group Call (RNA or Call waiting) on page 670
How to Delete a Group Call (RNA or Call Waiting) on page 670
How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting) on page 670
How to Enable or Disable Do Not Disturb for a Group Member on page 671

15.1.3 Hunt Group

Hunt groups permit the distribution of incoming calls to associated subscribers (members). If a subscriber is busy or does not accept an incoming call, the call is automatically forwarded to the next free member of the hunt group. All members of the hunt group can be reached at the same phone number.

Every member of a hunt group can also be reached at his or her own station number.

The hunt group must be assigned one of the following properties.

- Linear

  An inbound call is always signaled first at the first member of a hunt group. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.
- Cyclic

  An inbound call is always signaled first at the member that follows the subscriber who answered the last call. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.

The call is automatically forwarded to the next free hunt group member when the forwarding time expires, provided the call is not answered or a member is busy or DND is activated.

You can program a call forwarding destination (call destination list) if a call cannot be answered by any of the members of the hunt group.

A single station can belong to several groups simultaneously. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

The name assigned to the hunt group is shown on the internal caller's display. After a call is accepted, the name of the subscriber who accepted the call is displayed.

If a member has defined rules using the AutoAttendant, e.g., to forward calls, these rules will apply only to calls to his or her own station number. The rules are ignored for hunt group calls.

Up to 20 subscribers can be configured per hunt group.

Every hunt group can be assigned a name containing up to 16 characters.

Voicemail Box for Hunt Group

When setting up a hunt group, a voicemail box is automatically created for it. The call number of this voicemail box for the hunt group always matches that of the hunt group. If a call for a hunt group is not accepted by any member, the call is forwarded to the voicemail box for the hunt group. This requires the hunt group voicemail box to have been defined as the CFNA (call forwarding on no answer) destination of this hunt group.

If a member does not accept an incoming call to his or her own station number, this call is redirected to a call forwarding destination in accordance with the call destination list.

Example of a linear hunt group with the call number 404 and the members A (call number 200), B (201) and C (202). Call Forwarding-No Answer after Timeout to the voicemail box of the hunt group was set up for the hunt group. Every member has defined Call Forwarding-No Answer (CFNA) after Timeout to his or her own voicemail box.		
Inbound call for Member A (200)	All members are free.	Member A does not accept the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of member A.

	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is forwarded immediately (CFU) to the voicemail box of member A.
Inbound call for the hunt group (404)	All members are free.	The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined Call Forwarding Unconditional (CFU) to an external destination. Members B and C are free.	The call is signaled first at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.
	Member A has defined CFNA rules using the AutoAttendant. Members B and C are free.	The call is signaled first at member A, then at member B and then at member C. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the hunt group.

Activating/Deactivating the Hunt Group

If a subscriber is a member of a hunt group, he or she can use codes to leave and rejoin the hunt group.

If a subscriber is a member of both multiple hunt groups and multiple group calls, he or she can use codes to leave and rejoin all hunt groups and group calls. Subscribers are added to or removed from a specific hunt group or group call by entering codes and then making a selection from the hunt groups and group calls displayed.

You can also program function keys with a shift function for joining and leaving. You can program a function key here that applies for a specific or all hunt groups and group calls. Variable programming is also possible. After you press a function key of this kind, you must select one of the hunt groups and group calls displayed to define the hunt group or group call you want to leave/join.

Ring type

For every hunt group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in a hunt group.

INFO: No programming of function keys is possible for SIP phones. Specific display messages of a hunt group are not supported.

Dependencies

Topic	Dependency
Call forwarding	If a hunt group member activates call forwarding for all calls, all calls are signaled at the destination telephone.
Do Not Disturb	If a hunt group member activates the Do Not Disturb feature, incoming calls for his or her phone are not put through. This applies to calls for the hunt group and the member's own station number.
Queue	For cyclical and linear hunt groups, it is not possible to set up a call queue.
ISDN Phones	It is not possible to include ISDN telephones in hunt groups.

Related tasks

How to Add a Hunt Group on page 664
How to Change a Hunt Group on page 665
How to Delete a Hunt Group on page 666
How to Add or Delete a Member to or from a Hunt Group on page 667

15.1.4 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Wizards

Several different wizards are available to conveniently configure call pickup groups, group calls and hunt groups.

The **Call Pickup** wizard can be used to combine subscribers into a group to enable mutual call pickups. The following application cases, which can be configured using the wizard, are described here:

- How to Configure a Call Pickup Group

- How to Add or Delete a Member to or from a Call Pickup Group

The **Group Call / Hunt Group** wizard can be used to configure group calls of the type Group. The following application cases, which can be configured using the wizard, are described here:

- How to Add a Group Call (Group)
- How to Edit a Group Call (Group)
- How to Delete a Group Call (Group)
- How to Add or Delete a Member to or from a Group Call (Group)
- How to Add a Hunt Group
- How to Change a Hunt Group
- How to Delete a Hunt Group
- How to Add or Delete a Member to or from a Hunt Group

15.1.4.1 How to Configure a Call Pickup Group

The **Call Pickup** wizard enables you to combine subscribers into a group so that they can accept calls for one another.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Call Pickup** wizard. The list of all possible call pickup groups is displayed.
4) To configure a call pickup group, click **Edit** in the row containing the required call pickup group.
5) If you want to add members to the call pickup group, enable the **Allocation Group <Number>** check boxes for the desired call numbers/names.
6) If you want to remove members from the call pickup group, clear the **Allocation Group <Number>** check boxes for the desired call numbers/names.
7) Click on **OK** to accept the entries.
8) Enter the name of the just configured call pickup group in the **Name** field.
9) If you want to configure further call pickup groups, repeat steps 4 through 8.
10) Click on **OK & Next** followed by **Finish**.

Related concepts

Call Pickup Group on page 651

15.1.4.2 How to Add or Delete a Member to or from a Call Pickup Group

The **Group Pickup** wizard can be used to add or delete members to or from call pickup groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Call Pickup** wizard.
4) Click **Edit** in row of the desired call pickup group.
5) Select one of the following options:
   - If you want to add members to the call pickup group, enable the **Allocation Group <Number>** check boxes for the desired call numbers/ names.
   - If you want to remove members from the call pickup group, clear the **Allocation Group <Number>** check boxes for the desired call numbers/ names.
6) Click on **OK** to confirm the entries.
7) Click on **OK & Next** followed by **Finish**.

Related concepts

Call Pickup Group on page 651

15.1.4.3 How to Add a Group Call (Group)

The **Group Call / Hunt Group** wizard can be used to configure group calls of the type Group.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click on **Add** to set up a new group call.
5) Enter the call number of the new group call in the **Call number of the group** field.
6) Enter the DID number of the new group call in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

   ---

7) Enter the name of the new group call in the **Name of the group** field.
8) Select the item **Group** in the **Type** drop-down list.

9) Select one of the following options to transfer the call number for the group call into the internal directory:
   - If you do want the call number of the group call to appear in the internal directory, enable the **Tel. directory** check box.
   - If you do not want the call number of the group call to appear in the internal directory, clear the **Tel. directory** check box.
10) Select the call number of the desired subscriber from the **Call number of the subscriber to be added to the group** drop-down list.
11) Click on **OK & Next**.

> **INFO:** If the phone number and/or DID number you have selected already exists, you can call up the current dial plan (also called a numbering plan) to determine a free phone number and/or DID number.

12) Click **Edit** in the row containing the new group call to assign further subscribers to the group call.
13) Select the call number for the subscriber that you want to assign to the group call in the **Call No.** drop-down list.
14) Click on **Add**.
15) If you want to assign another subscriber to the group call, repeat steps 13 and 14.
16) Click on **OK** to accept the entries.
17) If you want to configure another group call, repeat steps 4 through 16.
18) Click on **OK & Next** followed by **Finish**.

Related concepts

Group Call on page 653

15.1.4.4 How to Edit a Group Call (Group)

The **Group Call / Hunt Group** wizard can be used to edit group calls of the type Group.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click **Edit** in the row containing the group call you want to change.
5) Change the required group parameters.

6) Only with UC Smart: Assign a mailbox to the group call if needed:
   a) Select whether the group call is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
   b) Only with default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
   c) Select a greeting from the **Greeting** drop-down list.
   d) If the password of the voicemail box is to be reset, select the **Password Reset** check box.

> **NOTICE:** The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

7) If you want to add a member to the group call, select the call number of the desired subscriber from the **Call No.** drop-down list and then click **Add**.
8) If you want to remove a member from the group call, click on **Clear** in the row of the group member to be removed and then on **OK**.
9) Click **OK** to confirm the entries.
10) Click **OK & Next** followed by **Finish**.

Related concepts

Group Call on page 653

15.1.4.5 How to Delete a Group Call (Group)

The **Group Call / Hunt Group** wizard can be used to delete group calls of the type Group.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click **Edit** in the row containing the group call you want to delete.
5) Click on **Delete Data**.
6) Click on **OK** to confirm the deletion.
7) Click on **OK & Next** followed by **Finish**.

Related concepts

Group Call on page 653

15.1.4.6 How to Add or Delete a Member to or from a Group Call (Group)

The **Group Call / Hunt Group** wizard can be used to add or delete members to or from group calls of the type Group.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click on **Edit** in the row of the desired system telephone.
5) Select one of the following options:
   - If you want to add a member to the group call, select the call number of the desired subscriber from the **Call No.** drop-down list and then click **Add**.
   - If you want to remove a member from the group call, click on **Clear** in the row of the group member to be removed and then on **OK**.
6) Click on **OK** to confirm the entries.
7) Click on **OK & Next** followed by **Finish**.

Related concepts

Group Call on page 653

15.1.4.7 How to Add a Hunt Group

The **Group Call / Hunt Group** wizard can be used to set up hunt groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click on **Add** to set up a new hunt group.
5) Enter the call number of the new hunt group in the **Call number of the group** field.
6) Enter the DID number of the new hunt group in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

   ---

7) Enter the name of the new hunt group in the **Group Name** field.

8) Select the type of the new hunt group in the **Type** drop-down list. You have the following options:
   - If you want a call to always be signaled at the first member of the hunt group first, then select the item **linear hunt group**.
   - If you want a call to always be signaled first at the hunt group member who follows the one who accepted the last call, select the item **cyclic hunt group**.
9) Select one of the following options to transfer the call number for the hunt group into the internal directory:
   - If you do want the call number of the hunt group to appear in the internal directory, enable the **Tel. directory** check box.
   - If you do not want the call number of the hunt group to appear in the internal directory, clear the **Tel. directory** check box.
10) Select the call number of the desired subscriber from the **Call number of the subscriber to be added to the group** drop-down list.
11) Click on **OK & Next**.

> **INFO:** If the phone number and/or DID number you have selected already exists, you can call up the current dial plan (also called a numbering plan) to determine a free phone number and/or DID number.

12) Click **Edit** in the row containing the new hunt group to assign further subscribers to the hunt group.
13) Select the call number of the subscriber that you want to assign to the hunt group in the **Call No.** drop-down list.
14) Click on **Add**.
15) If you want to assign another subscriber to the hunt group, repeat steps 13 and 14.
16) Click on **OK** to accept the entries.
17) If you want to configure another hunt group, repeat steps 4 through 16.
18) Click on **OK & Next** followed by **Finish**.

Related concepts

Hunt Group on page 656

15.1.4.8 How to Change a Hunt Group

The **Group Call / Hunt Group** wizard can be used to edit hunt groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click **Edit** in the row containing the hunt group you want to change.

5) Change the required hunt group parameters.
6) Only with UC Smart: Assign a mailbox to the hunt group if needed:
   a) Select whether the hunt group is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
   b) Only with default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
   c) Select a greeting from the **Greeting** drop-down list.
   d) If the password of the voicemail box is to be reset, select the **Password Reset** check box.

   NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.
7) If you want to add a member to the hunt group, select the call number of the desired subscriber from the **Call No.** drop-down list and then click **Add**.
8) If you want to remove a member from the hunt group, click on **Clear** in the row of the group member to be removed and then on **OK**.
9) If you want to change the position of the members within the hunt group, click **Change Order**. Enter the desired position number for each member in the **Position** field. Click **OK & Next**.
10) Click **OK** to confirm the entries.
11) Click **OK & Next** followed by **Finish**.

Related concepts

Hunt Group on page 656

15.1.4.9 How to Delete a Hunt Group

The **Group Call / Hunt Group** wizard can be used to delete hunt groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click **Edit** in the row containing the hunt group you want to delete.
5) Click on **Delete Data**.
6) Click on **OK** to confirm the deletion.
7) Click on **OK & Next** followed by **Finish**.

Related concepts

Hunt Group on page 656

15.1.4.10 How to Add or Delete a Member to or from a Hunt Group

The **Group Call / Hunt Group** wizard can be used to add or delete members to or from hunt groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Group Call / Hunt Group** wizard.
4) Click **Edit** in the row of the desired hunt group.
5) Select one of the following options:
   - If you want to add a member to the hunt group, select the call number of the desired subscriber from the **Call No.** drop-down list and then click **Add**.
   - If you want to remove a member from the hunt group, click on **Clear** in the row of the group member to be removed and then on **OK**.
6) Click on **OK** to confirm the entries.
7) Click on **OK & Next** followed by **Finish**.

Related concepts

Hunt Group on page 656

15.1.5 Configuring Call Pickup Groups, Group Calls and Hunt Groups using Expert Mode

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure call pickup groups, group calls and hunt groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- How to Enable or Disable the Display of a Caller's Station Number and Name
- How to Activate or Deactivate the Warning Tone
- How to Enable or Disable Call Pickup for Recalls
- How to Add a Group Call (RNA or Call Waiting)
- How to Display or Edit a Group Call (RNA or Call waiting)
- How to Delete a Group Call (RNA or Call Waiting)
- How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting)
- How to Enable or Disable Do Not Disturb for a Group Member

15.1.5.1 How to Enable or Disable the Display of a Caller's Station Number and Name

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **System Flags**.
4) Select one of the following options:
   - If you do want the call number and name of the caller to be displayed, enable the **Calling number in pick-up groups / ringing groups / CFN / RNA** check box.
   - If you do not want the call number and name of the caller to be displayed, clear the **Calling number in pick-up groups / ringing groups / CFN / RNA** check box.
5) Click on **Apply** followed by **OK**.

Related concepts

Call Pickup Group on page 651

15.1.5.2 How to Activate or Deactivate the Warning Tone

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **System Flags**.
4) Select one of the following options:
   - If you want to activate the warning tone, enable the check box **Warning signal for call pickup groups**.
   - If you want to deactivate the warning tone, clear the check box **Warning signal for call pickup groups**.
5) Click on **Apply** followed by **OK**.

Related concepts

Call Pickup Group on page 651

15.1.5.3 How to Enable or Disable Call Pickup for Recalls

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **System Flags**.
4) Select one of the following options:
   - If you want to allow a call pickup for recalls, enable the check box **Call Pickup after automatic recall**.
   - If you do not want to allow a call pickup for recalls, clear the check box **Call Pickup after automatic recall**.
5) Click on **Apply** followed by **OK**.

Related concepts

Call Pickup Group on page 651

15.1.5.4 How to Add a Group Call (RNA or Call Waiting)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click **Incoming Calls** > **Groups/Hunt groups** in the menu tree.
4) Click on the **Add Group** tab.
5) Enter the call number of the new group call in the **Phone Number** field.
6) Enter the DID number of the new group call in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

7) Enter the name of the new group call in the **Name** field.
8) Select one of the following options in the **Type** drop-down list:
   - If you want to set up a group call of type RNA (ring no answer), select the **RNA** entry.
   - If you want to set up a group call of type Call Waiting, select the **Call waiting** entry.
9) Select the call number for the subscriber that you want to assign to the group call from the **Phone Number** drop-down list.
10) Click on **Apply** followed by **OK**.

Related concepts

Group Call on page 653

15.1.5.5 How to Display or Edit a Group Call (RNA or Call waiting)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired group call.
4) Click on the **Edit Group Parameters** tab. The current settings of the group parameters are displayed.
5) Edit the desired parameters for the group call if required.
6) Click on **Apply** followed by **OK**.

Related concepts

Group Call on page 653

15.1.5.6 How to Delete a Group Call (RNA or Call Waiting)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired group call.
4) Click on the **Delete Group** tab.
5) Click on **Delete** followed by **OK**.

Related concepts

Group Call on page 653

15.1.5.7 How to Add or Delete a Member to or from a Group Call (RNA or Call Waiting)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to the group call, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired group

call. Then click on the **Add member** tab. Select the call number of the desired station in the **Phone Number** drop-down list. Then click **Apply**, followed by **OK**.

- To remove a member from the group call, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the group call ((Group Member) Call No, Name). Click on the **Delete Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Group Call on page 653

15.1.5.8 How to Enable or Disable Do Not Disturb for a Group Member

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) Navigate in the menu tree under **Stations** > **Station** > **…** down to the desired station (Index - Station Number - Name).
4) Click on the **Edit Station Flags** tab.
5) Select one of the following options:
   - If you want to enable the Do Not Disturb feature, select the check box **Call waiting rejection on**.
   - If you want to disable the Do Not Disturb feature, clear the **Call waiting rejection on** check box.

   NOTICE: When a group is configured as an Attendant group, all its' existing members are automatically set with the "Call waiting rejection flag" switched to false. This also applies to any new members of the Attendant group. The user can manually set "Call waiting rejection on" to true to any of the Attendant group's members in order to enable busy tone for this member, but this is not the default behavior.
6) Click on **Apply** followed by **OK**.

Related concepts

Group Call on page 653

15.2 Team Configuration / Team Group and Executive/Secretary / Top Group

A Team Configuration / Team Group offers several convenient team functions. The station numbers of all team members are programmed on MULAP keys (trunk keys). Every team member can thus access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks. An

Executive/Secretary or Top Group offers convenient Executive and Secretary functions (Top function) for up to three executives and up to three secretaries.

NOTICE: When creating a MULAP from Team/Top options in WBM / Manager E it is not allowed to enter any number beginning with ** or ***.

15.2.1 Team Configuration / Team Group

MULAP (Multiple Line Appearance) keys (trunk keys) are programmed on a telephone with team functions with the individual telephone's number and the phone numbers of all other team members. Every team member can access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks. In addition, DSS keys with which the team members can directly call one another are programmed automatically.

The MULAP keys give team members access to the phone numbers of all members. An incoming call for a team member can thus also be accepted by all other members by pressing the flashing MULAP key. Team members can also toggle between multiple trunks. By pressing a MULAP key, a team member can make an outbound call via the associated line. The station number of this line will then appear on the display of the called party.

Incoming calls are visually signaled at the same time on all team member phones via the MULAP key LED. You can also specify for each team member if incoming calls should also be signaled acoustically.

Every team member can use a group call key to activate or deactivate incoming call signaling for each individual trunk.

An administrator with the **Advanced** profile can configure up to 3 stations per Team configuration/Team group by using the **Team Configuration** wizard. An administrator with the **Expert** profile can configure up to ten stations per Team configuration or Team group in **Expert mode**.

An single subscriber may also simultaneously belong to several groups. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

Every team configuration / team group can be assigned a name containing up to 16 characters.

When setting up a Team configuration or Team group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**.):

- **Master**

  This parameter changes a member into a master of the Team configuration / Team group. If a master activates call forwarding, this applies to all members (phones) in the Team configuration / Team group.

  Default setting: master is the first member of the Team configuration / Team group.

- **Acoustic ring**

  If this parameter is activated, incoming calls are signaled acoustically.

  Default setting: the parameter is activated.
- **Automatic seizure outgoing**

  If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.

  Default setting: the parameter is activated.
- **No automatic incoming call acceptance**

  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **Automatic conference release**

  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **MULAP key set up**

  If the parameter is active, a MULAP key is programmed on the associated phone. Pressing the key sets up an outgoing call via the MULAP trunk of the master. The MULAP station number of the master appears on the called party's display.

  Default setting: the parameter is not activated.

Using MULAP Keys

Every team member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys (trunk keys) for every team member. This means that every team can use all available MULAP trunks.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slow: an on-hold call is waiting on the relevant trunk.

Using DSS Keys

Every team member has a DSS key for every other team member. This means that team members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the team member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: the associated Team member is not conducting a call.

- Lit: the associated Team member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Team member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated Team member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Ring type

For every Team configuration / Team group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

Fax Box for Team Configuration / Team Group

For each Team configuration or Team group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook.

If a fax box was already configured for the master (the first member) of the Team configuration/Team group, this fax box is taken over when setting up the Team configuration/Team group. Previously configured fax boxes of other members are deleted.

After a Team configuration or Team group is dissolved, only the prior master (i.e., the first member) can use his or her fax box.

Ordering of Mulap member devices

SIP telephones can be integrated in a Basic MULAP, as long as a TDM/HFA device has been defined as the first member of the Basic MULAP.IP telephones can be integrated in a Basic MULAP, as long as a TDM/HFA has been defined as the first member of the Basic MULAP.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/ UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

Mobility users, incl. GSM mobility users, Unify Phone and Microsoft Teams clients, can be integrated in a Basic MULAP, as long as a TDM/HFA device has been defined as the first member of the Basic MULAP.

NOTICE: The above extended description applies to both OpenScape Business X and OpenScape Business S systems, but limited to Team and Basic Mulap, and not subchapters with similar statements like Executive/Secretary / Top Group.

INFO: No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or

deactivated via codes. Specific display messages of the Basic MULAP are not supported.

NOTICE: High end phones, such as CP 400/600/600E/700/700X/710, keep their own journal entries and they have the capability to present more information. But regarding group configurations they rely on system data since the groups are configured on the system and not on the phones. As a result, information about groups might not be displayed in journal entries as they follow the system's limitations and configuration.

Dependencies

Topic	Dependency
Call forwarding	One team member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Team member activates the Do Not Disturb feature, incoming calls are not put through. **NOTICE:** An entire team is only busy, if all team members have activated the Do Not Disturb feature.
ISDN Phones	It is not possible to include ISDN telephones in Team configurations / Team groups.
Groups/Hunt groups	It is not possible to include a Basic/Executive MULAP master in Team configurations / Team groups.

Related concepts

Direct station select on page 610

Related tasks

How to Add a Team Configuration / Team Group on page 680
How to Edit a Team Configuration / Team Group on page 681
How to Delete a Team Configuration / Team Group on page 682
How to Add or Delete a Member to or from a Team Configuration or Team Group on page 686
How to Edit a Member of a Team Configuration / Team Group on page 686
How to Edit the Properties of Members in a Team Group on page 687
How to Change the Programmed Feature Keys for a Team Configuration / Team Group on page 687
How to Add a Fax Box to a Team Configuration / Team Group on page 688

15.2.2 Executive/Secretary or Top Group

Top groups can be configured if you need user-friendly executive and secretary functions (Top function).

Executive/secretary functions can be configured for groups with up to three executives and up to three secretaries.

INFO: The terms "executive" and "secretary" also apply to groups with more than one executive and more than one secretary. The terms "executive" and "secretary" used in this document are gender-neutral.

Every Top member (every executive and every secretary) is assigned a separate trunk, known as a MULAP (Multiple Line Appearance) trunk. The member's own MULAP trunk and the MULAP trunks of all other members are programmed as MULAP keys (trunk keys) for every Top member. The MULAP phone number is shown on the called party's display for outgoing calls via the MULAP trunk. The Secretary station can make calls via its own trunk or the MULAP trunk of all executives and other secretary stations. For example, if a connection is to be set up for an executive, the MULAP trunk of that executive can be used.

DSS keys are also programmed to allow the executive to call the secretary directly, and vice versa.

Incoming calls are visually signaled at the same time on all Top member phones via the LED on the trunk key. You can also specify for each Top member if incoming calls should also be signaled acoustically. Acoustic signaling depends here on the ring transfer key.

You can use a ring transfer key to change the signaling for incoming calls. Incoming calls are signaled either at the executive or secretary phone. If the executive presses the ring transfer key, incoming calls will still be displayed to the executive via a tray pop. Accepting a call can, however, only be done via an appropriate key on the phone and not via the tray pop.

You can use a group call key on Secretary phones to add or remove the station to or from the Executive/Secretary configuration or Top group. In this case, ring transfer has priority.

INFO: If the secretary uses the group call key to leave the Executive/Secretary configuration or Top group without activating ring transfer for the executive, incoming calls are not signaled at either the executive or the secretary.

An administrator with the **Advanced** profile can define up to two executives and two secretaries per Executive/Secretary configuration or Top group using the **Executive/Secretary** wizard. An administrator with the **Expert** profile can define up to three executives and three secretaries per Executive/Secretary configuration or Top group in **Expert mode**.

For every executive, a maximum of three phones can be set up; for every secretary, a maximum of two phones.

An single subscriber may also simultaneously belong to several groups. The following applies to groups of the type Group Call, Hunt Group, Team Configuration / Team Group and Executive/Secretary / Top Group: The sum of all the subscriber's memberships in these groups must not exceed 32.

Every Executive/Secretary configuration or Top group can be assigned a name containing up to 16 characters.

When setting up an Executive/Secretary configuration or Top group, the following properties are assigned to its members (these settings can be changed by an administrator with the **Expert** profile in **Expert mode**.):

- **Master**

  This parameter assigns executive functions to a member. The Executive MULAP trunk is automatically selected for a call on lifting the handset. Incoming calls via the associated Executive MULAP phone number are only signaled visually by default.

  Default setting: All executives of the Executive/Secretary configuration or Top group receive Executive functions.
- **Acoustic ring**

  If this parameter is activated, incoming calls are signaled acoustically.

  Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**

  If this parameter is active, a call is automatically made via the MULAP trunk of this member on lifting the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.

  Default setting: the parameter is activated for all members.
- **No automatic incoming call acceptance**

  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **Automatic conference release**

  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **MULAP key set up**

  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.

  Default setting: the parameter is activated.

Using MULAP Keys

Every Top member is assigned a separate trunk (MULAP trunk). The member's own trunk and the trunks of all other members are programmed as MULAP keys

(trunk keys) for every Top member. This means that every Top member can use all available MULAP lines.

The LED on a MULAP key (trunk key) can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Using DSS Keys

Every Top member has a DSS key for every other Top member. This means that Top members can reach each other directly at the push of a button.

A Direct Station Select (DSS) key can also be used to quickly transfer an existing call to the Top member programmed on it.

The LED on a DSS key can have different statuses with the following meanings:

- Off: The associated Top member is not conducting a call.
- Lit: the associated Top member is conducting a call or has activated Do Not Disturb.
- Flashing fast: the associated Top member is conducting a call. The call can be accepted by pressing the Direct Station Select (DSS) key.
- Flashing slowly: the associated Top member is being called and has not yet answered. The call can be accepted by pressing the Direct Station Select (DSS) key.

Ring type

For every Executive/Secretary configuration or Top group, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

Fax Boxes for Executive/Secretary Configuration or Top Group

For each member of an Executive/Secretary configuration or Top group, a fax box can be set up via which the members can receive Fax messages directly through myPortal for Desktop or myPortal for Outlook.

If a fax box was already configured for the first executive of the Executive/Secretary configuration or Top group, this fax box is taken over when setting up the Executive/Secretary configuration or Top group. Previously configured fax boxes of other members are deleted.

After an Executive/Secretary configuration or Top group is dissolved, only the prior first executive can use his or her fax box.

SIP Phones

SIP telephones can be integrated in an Executive/Secretary configuration or Top group. As a prerequisite, a system telephone (IP, HFA or SIP phone,

for example) must have been defined as the first member of the Executive/ Secretary configuration or Top group (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/ UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys and DSS keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive/Secretary configuration / Top group are not supported.

NOTICE: High end phones, such as CP600, keep their own journal entries and they have the capability to present more information. But regarding group configurations they rely on system data since the groups are configured on the system and not on the phones. As a result, information about groups might not be displayed in journal entries as they follow the system's limitations and configuration.

Dependencies

Topic	Dependency
Call forwarding	A Top member has activated call forwarding for all calls. In this case, all calls for his or her own station number will be forwarded.
Do Not Disturb	If a Top member activates the Do Not Disturb feature, incoming calls are not put through.
ISDN Phones	It is not possible to include ISDN or SIP phones in Executive/Secretary configurations or Top groups.
Groups/Hunt groups	It is not possible to include a Basic/Executive MULAP master in Executive/Secretary configurations or Top groups.

Related concepts

Direct station select on page 610

Related tasks

How to Add an Executive/Secretary or Top Group on page 683
How to Edit an Executive/Secretary or Top Group on page 684
How to Delete an Executive / Secretary or Top Group on page 685
How to Add or Delete a Member to or from an Executive/Secretary or Top Group on page 688
How to Edit a Member of an Executive/Secretary or Top Group on page 689
How to Edit the Properties of an Executive/Secretary or Top Group on page 689
How to Add a Fax Box to an Executive/Secretary or Top Group on page 690

15.2.3 Configuring Team Configurations / Team Groups and Executive/ Secretary Functions / Top Groups using Wizards

Several different wizards are available to conveniently configure team configurations (team groups) and executive/secretary functions (top groups).

The **Team Configuration** wizard can be used to set up Team configurations (Team groups). The following application cases, which can be configured using the wizard, are described here:

- How to Add a Team Configuration / Team Group
- How to Edit a Team Configuration / Team Group
- How to Delete a Team Configuration / Team Group

The **Executive / Secretary** wizard can be used to configure convenient Executive and Secretary functions (Top function). The following application cases, which can be configured using the wizard, are described here:

- How to Add an Executive/Secretary or Top Group
- How to Edit an Executive/Secretary or Top Group
- How to Delete an Executive / Secretary or Top Group

Related concepts

Configuring myPortal to go and Mobility Entry on page 908

15.2.3.1 How to Add a Team Configuration / Team Group

The **Team Configuration** wizard can be used to create Team configurations (Team groups).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Team Configuration** wizard.
4) Click on **Add** to set up a new team configuration.
5) Select the station number of the first telephone of the Team configuration in the **First Telephone** drop-down list.
6) Click on **OK & Next**.
7) In the **Name** field, enter the name of the new team configuration if no name is displayed or if you want to change the displayed name.

   Note: The **Name** field will already be preset with the name of the first telephone in the team configuration, provided a name was assigned to that telephone.

8) Enter the internal call number of the new team configuration in the **Internal Call Number** field if the displayed call number needs to be changed.

   The **Internal Number** field is already preset with the internal station number of the first telephone of the team configuration.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

9) Enter the DID number of the new team configuration in the **Direct inward dialing number** field if the displayed DID number needs to be changed.

   Note: The **Direct inward dialing number** field is already preset with the DID number of the first telephone of the team configuration.

10) Enter the internal number of the fax box for the new Team configuration under **Fax** in the **Internal Number** field if no call number is displayed or if the displayed call number needs to be changed.

    The **Internal Number** field will be preset with the internal number of the fax box of the first phone in the Team configuration if a fax box has already been configured for that phone.

11) Enter the DID number of the fax box for the new Team configuration under **Fax** in the **Direct inward dialing number** field if no DID number is displayed or if the displayed DID number needs to be changed.

    The **Direct inward dialing number** field will be preset with the DID number of the fax box of the first phone in the Team configuration if a fax box has already been configured for that phone.

12) Activate the **Team as group member** flag.

    The **Team as group member** flag is configurable only when the Team Group has members with the same station type, which results in a single MULAP group. When this flag is activated, the MULAP group can be added as a member in Groups.

13) Select the station number of the second telephone of the new Team configuration from the **Second Telephone** drop-down list.

14) Select the station number of the third telephone of the Team configuration from the **Third Telephone** drop-down list.

15) Click on **OK & Next**.

16) If you want to configure another Team configuration, repeat steps 4 through 15.

17) Click on **OK & Next** followed by **Finish**.

Related concepts

Team Configuration / Team Group on page 672

15.2.3.2 How to Edit a Team Configuration / Team Group

The **Team Configuration** wizard can be used to edit Team configurations (Team groups).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Team Configuration** wizard.
4) Click **Edit** in the row of the team configuration you want to change.
5) Change the required parameters.
6) Only with UC Smart: Assign a mailbox to the team configuration if needed:
   a) Select whether the team configuration is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
   b) Only with default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
   c) Select a greeting from the **Greeting** drop-down list.
   d) If the password of the voicemail box is to be reset, select the **Password Reset** check box.

   NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.
7) Click **OK & Next**.
8) Click on **OK & Next** followed by **Finish**.

Related concepts

Team Configuration / Team Group on page 672

15.2.3.3 How to Delete a Team Configuration / Team Group

The **Team Configuration** wizard can be used to delete Team configurations (Team groups).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Team Configuration** wizard.
4) Click **Edit** in the row of the team configuration you want to delete.
5) Click on **Delete Data**.
6) Click on **OK** to confirm the deletion.

7) Click on **OK & Next** followed by **Finish**.

NOTICE: In applications using CSTA interface (UC, OSCC, etc.) when a Team Group or a member of a Team Group is deleted, a system restart is needed.

Related concepts

Team Configuration / Team Group on page 672

15.2.3.4 How to Add an Executive/Secretary or Top Group

The **Executive / Secretary** wizard can be used to configure user-friendly executive and secretary functions (Top function).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Executive / Secretary** wizard.
4) Click on **Add** to set up a new Executive/Secretary configuration (Top group).
5) Enter the name of the new Executive/Secretary configuration in the **Name** field.
6) Select the desired call numbers for the new Executive/Secretary configuration in the associated drop-down lists.
7) Click on **OK & Next**.
8) Enter the internal number of the fax box for the new Executive/Secretary configuration under **Fax** in the **Call No.** field if no call number is displayed or if the displayed call number needs to be changed.

   The **Call No.** field will be preset with the internal number of the fax box of the first executive in the Executive/Secretary configuration if a fax box has already been configured for this phone.
9) Enter the DID number of the fax box for the new Executive/Secretary configuration under **Fax** in the **DID** field if no DID number is displayed or if the displayed direct inward dialing number needs to be changed.

   The **Direct inward dialing** field will be preset with the DID number of the fax box of the first executive in the Executive/Secretary configuration if a fax box has already been configured for this phone.

INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

10) Select a default for the key assignment:
    - If the keys for the Executive/Secretary functions are to be set up on the first or second add-on device, enable the check box **to first/second console**.
    - If the keys for the Executive/Secretary functions are to be set up on the first free function keys of the telephone, enable the check box **to first free key**.
11) Click on **OK & Next**.
12) If you want to configure another Executive/Secretary configuration, repeat steps 4 through 11.
13) Click on **OK & Next** followed by **Finish**.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.3.5 How to Edit an Executive/Secretary or Top Group

The **Executive / Secretary** wizard can be used to edit convenient Executive and Secretary functions (Top function).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Executive / Secretary** wizard.
4) Click **Edit** in the row containing the Executive/Secretary configuration you want to change.
5) Change the required parameters.
6) Only with UC Smart: Assign a mailbox to the Top Group if needed:
    a) Select whether the Top Group is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.
    b) Only with default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.
    c) Select a greeting from the **Greeting** drop-down list.
    d) If the password of the voicemail box is to be reset, select the **Password Reset** check box.

    NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.
7) Click **OK & Next**.
8) Edit the desired entries for the fax box (**Fax**) and the **Key assignment**.

9) Click **OK & Next**.
10) Click **OK & Next** followed by **Finish**.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.3.6 How to Delete an Executive / Secretary or Top Group

The **Executive / Secretary** wizard can be used to delete convenient Executive and Secretary functions (Top function).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Executive / Secretary** wizard.
4) Click **Edit** in the row containing the Executive/Secretary configuration (Top group) you want to delete.
5) Click on **Delete Data**.
6) Click on **OK** to confirm the deletion.
7) Click on **OK & Next** followed by **Finish**.

NOTICE: In applications using CSTA interface (UC, OSCC, etc.) when an Executive/Secretary or Top group or a member of an Executive/Secretary or Top group is deleted, a system restart is needed.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.4 Configuring Team configurations / Team groups and Executive/ Secretary functions / Top groups using Expert mode

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional options to configure Team configurations / Team groups and Executive/Secretary functions / Top groups via the **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- How to Add or Delete a Member to or from a Team Configuration or Team Group
- How to Edit a Member of a Team Configuration / Team Group
- How to Edit the Properties of Members in a Team Group

- How to Change the Programmed Feature Keys for a Team Configuration / Team Group
- How to Add a Fax Box to a Team Configuration / Team Group
- How to Add or Delete a Member to or from an Executive/Secretary or Top Group
- How to Edit a Member of an Executive/Secretary or Top Group
- How to Edit the Properties of an Executive/Secretary or Top Group
- How to Add a Fax Box to an Executive/Secretary or Top Group

15.2.4.1 How to Add or Delete a Member to or from a Team Configuration or Team Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

INFO: The **Team Configuration** wizard can be used by an administrator with the **Advanced** profile to define up to three members (phones) for a Team configuration (Team group). Additional members must be added by an administrator with the **Expert** profile in **Expert mode** (see the description below).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to the Team group, navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired Team group. Click on the **Add Team/top Member** tab. Select the station type in the **Type** drop-down list and select the call number of the desired station in the **Call No.** drop-down list. Then click **Apply**, followed by **OK**.
   - To remove a member from the Team group, navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired member of the Team group (Group Member, Call No, Name). Click on the **Delete Team/top Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Team Configuration / Team Group on page 672

15.2.4.2 How to Edit a Member of a Team Configuration / Team Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.

3) Navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to a member of the Team group ((Group member) Station Number, Name).
4) Click on the **Edit Team/Top Member** tab.
5) Change the required parameters.
6) Click on **Apply** followed by **OK**.

Related concepts

Team Configuration / Team Group on page 672

15.2.4.3 How to Edit the Properties of Members in a Team Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to a member of the Team group ((Group member) Station Number, Name).
4) Click on the **Edit Team/Top Group Parameters** tab.
5) Change the required properties.
6) Click on **Apply** followed by **OK**.

Related concepts

Team Configuration / Team Group on page 672

15.2.4.4 How to Change the Programmed Feature Keys for a Team Configuration / Team Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired Team group).
4) Click on the **Edit Team/top Group** tab.
5) Select a default for the key assignment:
   - If the keys are to be set up on the first or second add-on device, enable the check box **to first/second console**.
   - If the keys are to be set up on the first free function keys of the telephone, enable the check box **to first free key**.
6) Click on **Apply** followed by **OK**.

Related concepts

Team Configuration / Team Group on page 672

15.2.4.5 How to Add a Fax Box to a Team Configuration / Team Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired Team group).
4) Click on the **Add Fax Box** tab.
5) Enter the internal call number of the fax box in the **Fax No.** field of the desired Team group member.
6) Enter the direct inward dialing number of the fax box in the **Fax DID** field of the desired Team group member.
7) Click on **Apply** followed by **OK**.

Related concepts

Team Configuration / Team Group on page 672

15.2.4.6 How to Add or Delete a Member to or from an Executive/Secretary or Top Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

INFO: The **Executive / Secretary** wizard can be used by an administrator with the **Advanced** profile to define up to two executives and two secretaries per Executive/Secretary configuration (Top group). Additional members must be added by an administrator with the **Expert** profile in **Expert mode** (see the description below).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to the Top group (Executive/Secretary configuration), navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired Top group (Executive/Secretary configuration). Click on the **Add Team/top Member** tab. Select the station type in the **Type** drop-down list and select the call number of the desired station in the **Call No.** drop-down list. Then click **Apply**, followed by **OK**.

- To remove a member from the Top group (Executive/Secretary configuration), navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired member of the Top group (Executive/Secretary configuration) (Group Member, Call No, Name). Click on the **Delete Team/top Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.4.7 How to Edit a Member of an Executive/Secretary or Top Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/Top** > **…** down to a member of the Top group (Executive/Secretary configuration) ((Group member) Station Number, Name).
4) Click on the **Edit Team/Top Member** tab.
5) Change the required parameters.
6) Click on **Apply** followed by **OK**.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.4.8 How to Edit the Properties of an Executive/Secretary or Top Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/Top** > **…** down to a member of the Top group (Executive/Secretary configuration) ((Group member) Station Number, Name).
4) Click on the **Edit Team/Top Group Parameters** tab.
5) Change the required properties.
6) Click on **Apply** followed by **OK**.

Related concepts

Executive/Secretary or Top Group on page 676

15.2.4.9 How to Add a Fax Box to an Executive/Secretary or Top Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Team/top** > **…** down to the desired Top group (Executive/Secretary configuration).
4) Click on the **Add Fax Box** tab.
5) Enter the internal call number of the fax box in the **Fax No.** field of the desired Top group (or Executive/Secretary configuration) member.
6) Enter the direct inward dialing number of the fax box in the **Fax No.** field of the desired Top group (or Executive/Secretary configuration) member.
7) Click on **Apply** followed by **OK**.

Related concepts

Executive/Secretary or Top Group on page 676

15.3 Basic MULAP and Executive MULAP

A Basic MULAP enables a subscriber who uses multiple telephones (e.g., a fixed-network telephone and a mobile phone) to be reached under a single phone number. You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

15.3.1 Basic MULAP

Basic MULAPs can be configured if a subscriber is using a number of different phones (for example, a fixed-network phone and mobile phone) but would like to be reached at a single phone number (Basic MULAP phone number).

If a caller rings the Basic MULAP phone number, the call is visually signaled at all phones belonging to the Basic MULAP. The subscriber can also set whether or not incoming calls should also be acoustically signaled for each individual member. The status of the Basic MULAP changes to busy and other callers hear the busy signal when a call is answered.

The Basic MULAP phone number is shown on the called party's display for outgoing calls via the Basic MULAP trunk.

Up to 20 members can be configured per Basic MULAP.

Every Basic MULAP can be assigned a name containing up to 16 characters.

Each of the subscriber's phones is a member of the Basic MULAP and each member can be assigned the following properties:

- **Master**

  This parameter changes a member into a master of the Basic MULAP. If a master activates call forwarding, this feature applies to all members (phones)

in the Basic MULAP. If the master activates an automatic callback on a Basic MULAP, the callback is initiated as soon as all masters are free.

A subscriber may not be included as a MULAP master in hunt groups more than 25 times.

Default setting: master is the first member of the Basic MULAP.

- **Acoustic ring**

  If this parameter is activated, incoming calls are signaled acoustically.

  Default setting: the parameter is active for all masters.
- **Automatic seizure outgoing**

  If this parameter is active, the Basic MULAP trunk is automatically called when the subscriber lifts the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.

  Default setting: automatic outgoing seizure is assigned to all masters.
- **No automatic incoming call acceptance**

  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **Automatic conference release**

  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **MULAP key set up**

  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Basic MULAP trunk. The Basic MULAP number appears on the called party's display.

  Default setting: the parameter is activated.

Number/Name Display

When an outgoing call is set up, a station number is assigned (local station number or MULAP group number).

When an incoming MULAP call is answered, the MULAP group number is assigned.

In the case of calls to a MULAP:

- Before the call is answered, the display of the calling party shows the MULAP name and/or MULAP number being called.
- After the call is answered, the display of the calling party shows the station name and/or MULAP number of the answering party.
- In the case of calls from a MULAP station (MULAP key or preference), the display of the called and answering parties always shows the station name and/or MULAP number..
- The following generally applies to outgoing seizures: If a station conducts a call using the local station number and the outgoing preference differs from

the local station number, the display of the called party always shows the station number of the outgoing preference.

Using MULAP Keys

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Ring type

For every Basic MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

Ordering of Mulap member devices

SIP telephones can be integrated in a Basic MULAP, as long as a TDM/HFA device has been defined as the first member of the Basic MULAP.IP telephones can be integrated in a Basic MULAP, as long as a TDM/HFA has been defined as the first member of the Basic MULAP.

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/ UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

Mobility users, incl. GSM mobility users, Unify Phone and Microsoft Teams clients, can be integrated in a Basic MULAP, as long as a TDM/HFA device has been defined as the first member of the Basic MULAP.

NOTICE: The above extended description applies to both OpenScape Business X and OpenScape Business S systems, but limited to Team and Basic Mulap, and not subchapters with similar statements like Executive/Secretary / Top Group.

INFO: No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Basic MULAP are not supported.

Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Basic MULAPs.

Related tasks

How to Add a Basic MULAP on page 696
How to Display or Edit a Basic MULAP on page 696
How to Delete a Basic MULAP on page 697
How to Add or Delete a Member to or from a Basic MULAP on page 697
How to Edit a Member of a Basic MULAP on page 698

15.3.2 Executive MULAP

You can configure Executive MULAPs if you want to use restricted executive and secretary functions.

All members of an Executive MULAP can be reached at the Executive MULAP phone number as well as at their personal station numbers.

INFO: The terms "executive" and "secretary" used in this document are gender-neutral.

Up to 20 members can be configured per Executive MULAP.

Every Executive MULAP can be assigned a name containing up to 16 characters.

The parameters described below define which members of an Executive MULAP can use executive functions (Executive) and which can use secretary functions (Secretary).

If a caller rings the Executive MULAP phone number, the call is visually signaled at all phones belonging to the Executive MULAP. Incoming calls are also signaled acoustically for members with secretary functions.

The Executive MULAP phone number is shown on the called party's display for outgoing calls via the Executive MULAP trunk.

The members of an Executive MULAP can be assigned the following properties:

- **Master**

  This parameter is used to assign executive functions to a member. The Executive MULAP trunk is automatically selected for a call when you lift the handset. Incoming calls via the Executive MULAP phone number are only signaled visually.

  A subscriber may not be included as a MULAP master in hunt groups more than 25 times.

  Default setting: the first member of the Executive MULAP is assigned executive functions.

- **Acoustic ring**

  If this parameter is activated, incoming calls are signaled acoustically.

  Default setting: the parameter is active for all members with the secretary function.
- **Automatic seizure outgoing**

  If this parameter is active, the Executive MULAP trunk is automatically called when you lift the handset. If the parameter is not active, the subscriber must press the MULAP key before dialing is possible.

  This parameter cannot be used by members with the secretary function.

  Default setting: the parameter is active for all members with the executive function.
- **No automatic incoming call acceptance**

  If this parameter is activated, you cannot answer an incoming call by lifting the handset. An incoming call must be accepted by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **Automatic conference release**

  If the parameter is active, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key.

  Default setting: the parameter is not activated.
- **MULAP key set up**

  If the parameter is active, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display.

  Default setting: the parameter is activated.

Using MULAP Keys

The LED on a MULAP key can have different statuses with the following meaning:

- Off: the relevant trunk is free and can be used.
- Lit: the relevant trunk is busy.
- Flashing fast: call on the relevant trunk.
- Flashing slowly: an on-hold call is waiting on the relevant trunk or the relevant trunk was released for a conference.

Ring type

For every Executive MULAP, an administrator with the **Expert** profile can define the acoustic signaling of incoming external calls via the ring type setting. You have the following options:

- Two rings (default setting)
- Three rings
- short-long-short ring

Only the default setting is possible for analog phones. Changes have no effect.

SIP Phones

SIP telephones can be integrated in an Executive MULAP. As a prerequisite, a system telephone (HFA or UP0 phone, for example) must have been defined as the first member of the Executive MULAP (Exec. 1).

Dual-mode mobile phones that are configured as Mobility Entry stations, for example, can be integrated. Dual-mode mobile phones support both GSM/ UMTS networks and WLAN networks. A dual-mode mobile phone can be registered as an IP station (SIP client) at the communication system over a WLAN.

INFO: No programming of MULAP keys is possible for SIP phones. Furthermore, no features can be activated or deactivated via codes. Specific display messages of the Executive MULAP are not supported.

Dependencies

Topic	Dependency
Do Not Disturb	When Do Not Disturb is activated, incoming calls are no longer put through.
ISDN Phones	It is not possible to include ISDN telephones in Executive MULAPs.

Related tasks

How to Add an Executive MULAP on page 698
How to Display or Edit an Executive MULAP on page 699
How to Delete an Executive MULAP on page 699
How to Add or Delete a Member to or from an Executive MULAP on page 699
How to Edit a Member of an Executive MULAP on page 700

15.3.3 Configuring Basic MULAPs and Executive MULAPs

The configuration of Basic and Executive MULAPs can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- How to Add a Basic MULAP
- How to Display or Edit a Basic MULAP
- How to Delete a Basic MULAP
- How to Add or Delete a Member to or from a Basic MULAP
- How to Edit a Member of a Basic MULAP
- How to Add an Executive MULAP
- How to Display or Edit an Executive MULAP
- How to Delete an Executive MULAP
- How to Add or Delete a Member to or from an Executive MULAP
- How to Edit a Member of an Executive MULAP

15.3.3.1 How to Add a Basic MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click **Incoming Calls** > **Groups/Hunt groups** in the menu tree.
4) Click on the **Add Group** tab.
5) Enter the call number of the new Basic MULAP in the **Call number** field.
6) Enter the DID number of the new Basic MULAP in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

7) Enter the name of the new Basic MULAP in the **First Name** and **Last Name** fields.
8) Select **Basic MULAP** in the **Type** drop-down list.
9) Select the call number for the subscriber that you want to assign to the Basic MULAP group from the **Call number** drop-down list.
10) Click on **Apply** followed by **OK**.

    NOTICE: In applications using CSTA interface (UC, OSCC, etc.) when a Basic MULAP group or a member of a Basic MULAP group is created, a system restart is needed.

Related concepts

Basic MULAP on page 690

15.3.3.2 How to Display or Edit a Basic MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Basic MULAP.
4) Click on the **Edit Group Parameters** tab. The current settings of the group parameters are displayed.
5) Edit the desired parameters for the Basic MULAP if required.
6) Click on **Apply** followed by **OK**.

Related concepts

Basic MULAP on page 690

15.3.3.3 How to Delete a Basic MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Basic MULAP.
4) Click on the **Delete Group** tab.
5) Click on **Delete** followed by **OK**.

NOTICE: In applications using CSTA interface (UC, OSCC, etc.) when a Basic MULAP group or a member of a Basic MULAP group is deleted, a system restart is needed.

Related concepts

Basic MULAP on page 690

15.3.3.4 How to Add or Delete a Member to or from a Basic MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to a Basic MULAP, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Basic MULAP. Click on the **Add Member** tab. Select the call number of the desired station in the **Phone Number** drop-down list. Then click **Apply**, followed by **OK**.
   - To remove a member from a Basic MULAP, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the Basic MULAP ((Group Member) Call No, Name). Click on the **Delete Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Basic MULAP on page 690

15.3.3.5 How to Edit a Member of a Basic MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the Basic MULAP ((Group member) Station Number, Name).
4) Click on the **Edit Member** tab.
5) Change the required parameters.
6) Click on **Apply** followed by **OK**.

Related concepts

Basic MULAP on page 690

15.3.3.6 How to Add an Executive MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click **Incoming Calls** > **Groups/Hunt groups** in the menu tree.
4) Click on the **Add Group** tab.
5) Enter the call number of the new Executive MULAP in the **Call number** field.
6) Enter the DID number of the new Executive MULAP in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

7) Enter the name of the new Executive MULAP in the **First name** and **Last name** fields.
8) Select **Executive MULAP** in the **Type** drop-down list.
9) Select the call number for the subscriber that you want to assign to the Executive MULAP group from the **Call number** drop-down list.
10) Click on **Apply** followed by **OK**.

Related concepts

Executive MULAP on page 693

15.3.3.7 How to Display or Edit an Executive MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Executive MULAP.
4) Click on the **Edit Group Parameters** tab. The current settings of the group parameters are displayed.
5) Edit the desired parameters for the Executive MULAP if required.
6) Click on **Apply** followed by **OK**.

Related concepts

Executive MULAP on page 693

15.3.3.8 How to Delete an Executive MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Executive MULAP.
4) Click on the **Delete Group** tab.
5) Click on **Delete** followed by **OK**.

NOTICE: In applications using CSTA interface (UC, OSCC, etc.) when an Executive MULAP group or a member of an Executive MULAP group is deleted, a system restart is needed.

Related concepts

Executive MULAP on page 693

15.3.3.9 How to Add or Delete a Member to or from an Executive MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to an Executive MULAP, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired Executive MULAP. Click on the **Add Member** tab. Select the call number of the desired station in the **Phone Number** drop-down list. Then click **Apply**, followed by **OK**.
   - To remove a member from an Executive MULAP, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the Executive MULAP ((Group Member) Call No, Name). Click on the **Delete Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Executive MULAP on page 693

15.3.3.10 How to Edit a Member of an Executive MULAP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the Basic MULAP ((Group member) Station Number, Name).
4) Click on the **Edit Member** tab.
5) Change the required parameters.
6) Click on **Apply** followed by **OK**.

Related concepts

Executive MULAP on page 693

15.3.3.11 How to Add a Basic MULAP in a Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Incoming Calls**.
3) Click to the desired Basic MULAP, in the menu tree under **Incoming calls > Groups/Hunt groups**.

4) Click on **Edit Group parameters** tab. The current settings of the group parameters are displayed.
5) Activate the **Mulap as group member** flag.
6) Click on the desired Group in the menu tree under **Incoming calls > Groups/Hunt groups** to add a Basic MULAP as a member in the Group.
7) Click on **Add Member** tab and select the Basic MULAP from the drop down menu in the **Call number** field.
8) Click on **Apply** followed by **OK**.

Restrictions:

- All the Basic MULAP members must be configured with M, R, A parameters.
- The maximum number of the Group members must be up to 20, including the members of the Basic MULAP.
- The Basic MULAP members cannot already be members of the Group.
- It is allowed to add a MULAP to:
  1) Linear hunt group
  2) Cyclical hunt group
  3) Group
- It is not allowed to add a MULAP to:
  1) Call waiting
  2) RNA
- A group cannot be changed to Call waiting or RNA if it contains a MULAP.

15.4 Voicemail Group and Fax Box Group

A voicemail group enables a subscriber group to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. A fax box group (fax group) enables a subscriber group to access fax messages. The fax box of the group is reached directly via the station number of the fax box group.

15.4.1 Voicemail Group

A voicemail group enables a specific group of subscribers to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. After a voicemail is left in the voicemail box of the group, it is forwarded to the voicemail boxes of all members.

All members receive the voicemail simultaneously. Whenever a member deletes a voicemail, this voicemail is also deleted from the voicemail boxes of all members and the voicemail box of the group. The personal voicemails of all members are not affected by this.

Every member of a voicemail group can be reached under his or her own station number.

Up to 20 members can be configured per voicemail group.

Every voicemail group can be assigned a name containing up to 16 characters.

At least one member of a voicemail group requires a Voicemail license.

Dependencies

Topic	Dependency
Ringing group on	The *Ringing group* feature cannot be used.

Related tasks

How to Add a Voicemail Group on page 703
How to Display or Edit a Voicemail Group on page 703
How to Delete a Voicemail Group on page 704
How to Add or Delete a Member to a Voicemail Group on page 704
How to Edit a Member of a Voicemail Group on page 704

15.4.2 Fax Box Group

A fax box group (fax group) enables a specific group of subscribers to access fax messages. The fax box of the group is reached directly via the station number of the fax box group. After a fax message is left in the fax box of the group, it is forwarded to the fax boxes of all members.

All members receive the fax message simultaneously. Whenever a member deletes a fax message, this voicemail is also deleted from the fax boxes of all members and the fax box of the group.

Every member of a fax box group can be reached under his or her own station number.

Up to 20 fax box groups can be configured.

Every fax box group can be assigned a name containing up to 16 characters.

At least one member of a fax box group requires a Fax license.

Related tasks

How to Configure a Fax Box Group on page 705
How to Display or Edit a Fax Box Group on page 706
How to Add or Delete a Member to a Fax Box Group on page 706

15.4.3 Configuring Voicemail Box Groups and Fax Box Groups

The configuration of voicemail box groups and fax box groups can only be performed by an administrator with the **Expert** profile and in **Expert mode**.

The procedure for the following application cases, which can be configured using the **Expert mode** wizard, is described here:

- How to Add a Voicemail Group
- How to Display or Edit a Voicemail Group
- How to Delete a Voicemail Group
- How to Add or Delete a Member to a Voicemail Group
- How to Edit a Member of a Voicemail Group
- How to Configure a Fax Box Group

- How to Display or Edit a Fax Box Group
- How to Delete a Fax Box Group
- How to Add or Delete a Member to a Fax Box Group

15.4.3.1 How to Add a Voicemail Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click **Incoming Calls** > **Groups/Hunt groups** in the menu tree.
4) Click on the **Add Group** tab.
5) Enter the call number of the new voicemail group in the **Phone Number** field.
6) Enter the DID number of the new voicemail group in the **Direct inward dialing number** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

7) Enter the name of the new voicemail group in the **Name** field.
8) Select the item **Voicemail** in the **Type** drop-down list.
9) Select the call number for the subscriber that you want to assign to the new voicemail group from the **Phone Number** drop-down list.
10) Click on **Apply** followed by **OK**.

Related concepts

Voicemail Group on page 701

15.4.3.2 How to Display or Edit a Voicemail Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired voicemail group.
4) Click on the **Edit Group Parameters** tab. The current settings of the group parameters are displayed.
5) Edit the desired parameters for the voicemail group if required.
6) Click on **Apply** followed by **OK**.

Related concepts

Voicemail Group on page 701

15.4.3.3 How to Delete a Voicemail Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired voicemail group.
4) Click on the **Delete Group** tab.
5) Click on **Delete** followed by **OK**.

Related concepts

Voicemail Group on page 701

15.4.3.4 How to Add or Delete a Member to a Voicemail Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Select one of the following options:
   - To add a member to a voicemail group, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired voicemail group. Click on the **Add Member** tab. Select the call number of the desired station in the **Phone Number** drop-down list. Then click **Apply**, followed by **OK**.
   - To remove a member from a voicemail group, navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the voicemail group ((Group Member) Call No, Name). Click on the **Delete Member** tab. Click on **Delete** followed by **OK**.

Related concepts

Voicemail Group on page 701

15.4.3.5 How to Edit a Member of a Voicemail Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **Groups/Hunt groups** > **…** down to the desired member of the Voicemail group ((Group member) Station Number, Name).
4) Click on the **Edit Member** tab.
5) Change the required parameters.
6) Click on **Apply** followed by **OK**.

Related concepts

Voicemail Group on page 701

15.4.3.6 How to Configure a Fax Box Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Station**.
3) In the menu tree, click **Stations** > **UC Applications** > **Fax Group**. The already configured fax box groups are displayed.
4) Select the next free row and enter the call number of the new fax box group in the **Phone Number** field.
5) Enter the DID number of the new fax box group in the **DID** field.

   INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

6) Enter the name of the new fax box group in the **Name** field.
7) Select the item **Fax Group** in the **Type** drop-down list.
8) Click **Apply** followed by **OK**.
9) Close the **Fax Group** window.
10) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
11) Click **Groups**.
12) Click on the **Fax Group** tab.
13) Select the new fax box group and click **Edit**.
14) Select one of the following options:
    - If you want to add a member to a fax box group, mark the desired member in the **Users** list.
    - If you want to add several members to the fax box group, press the <Ctrl> key and select the desired members in the **Users** list.
15) Click **Save**.

Related concepts
Fax Box Group on page 702

15.4.3.7 How to Display or Edit a Fax Box Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Station**.
3) In the menu tree, click **Stations** > **UC Applications** > **Fax Group**.
4) Click on the desired fax box group in the menu tree.
5) Click the **Edit Station Parameters** tab.
6) Edit the desired parameters for the fax box group if required.
7) Click **Apply** followed by **OK**.

Related concepts
Fax Box Group on page 702

15.4.3.8 How to Delete a Fax Box Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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 How to Add or Delete a Member to a Fax Box Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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) Select one of the following options:
   - 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) Click on **Save**.

Related concepts

Fax Box Group on page 702

15.5 Speaker Call for Groups

Speaker call for groups enable the broadcasting of announcements to all internal members of a group.

15.5.1 Internal Paging

Internal paging enables internal members of a group to be addressed directly. This feature is also known as a group broadcast. Internal paging is not performed for group members who are busy or have activated the Do Not Disturb feature. Group members have no direct answering option. Answering is only possible by lifting the handset, which results in a transition to a normal two-way conversation.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Internal Paging" feature cannot be used with ISDN or SIP phones.

15.5.2 Transfer to Group from Announcement

A call on consultation hold can be transferred to a group via Transfer from Announcement. An announcement to the group is initiated for this (internal paging). The system sets up a two-party call when another party in the group lifts the handset or turns on the loudspeaker and the party who transferred the call hangs up. The connection is cleared down for the other group members.

Internal paging can be used via a function key programmed for this purpose, the menu item **Speaker call** or by entering the appropriate code and then dialing the station number of the target group. A function key can also be programmed with a group phone number. A connection to the programmed group is immediately set up when you press a function key of this kind.

Dependencies

Topic	Dependency
Do Not Disturb	Group members who have activated DND do not receive any announcements.
ISDN phones, SIP phones	The "Transfer to Group from Announcement" feature cannot be used with ISDN and SIP phones.

15.6 UCD (Uniform Call Distribution)

The Uniform Call Distribution (UCD) feature of the communication system enables incoming calls to be uniformly distributed to a group of stations (UCD-group).

UCD groups are primarily used in technical hotline environments (e.g., customer service hotlines), for managing complaints, in market research, order processing and acceptance (e.g., by mail-order companies and ticketing services) and even for emergency services.

As a rule, call distribution occurs by sending an incoming call to a UCD group to the station (agent) in the UCD group whose last call lies furthest in the past. It is also possible to define other distribution rules.

If there is no agent free to accept an incoming call, the call is automatically forwarded to a queue. Waiting calls are distributed to free agents on the basis of priority and wait time.

Announcements or music on hold can be played for waiting callers.

Configuration

The **UCD** wizard can be used to configure groups and stations for intelligent call distribution (UCD). The following application cases, which can be configured using the wizard, are described here:

- How to Configure Call Distribution / UCD Groups
- How to Add or Delete UCD Agents
- How to Change Announcements / Music on Hold for UCD

Besides the configuration options available through wizards, administrators with the **Expert** profile are also offered additional configuration options in **Expert mode**.

15.6.1 Call Distribution / UCD Group

A UCD group contains agents (subscribers) that belong to a work group and can be reached at a single phone number. An incoming internal or external call is automatically delivered to the agent who is idle longest.

Every UCD group can be configured using the WBM (**in Expert mode**) so that incoming calls to an agent are automatically accepted by the communication system (Unattended Incoming Call Connection AICC).

If all agents of a UCD group are busy, incoming calls can be placed in a queue. The maximum number of calls in the queue can be individually set for every UCD group. When the maximum number of queued calls is reached, further calls can be forwarded to an overflow destination (which may be an external destination, another UCD group, an internal station or a group).

If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

Announcements or music can be played for on-hold callers.

Every UCD group can be assigned a name containing up to 16 characters.

Dependencies

Topic	Dependency
Call forwarding	A call is not forwarded to a UCD group in the following cases: • If a hunt group is called and a subscriber with call forwarding to a UCD group is next, this call is not forwarded. In this case, the next station in the hunt group is immediately called. • A subscriber is a member of a group call with the property "Group" and has activated call forwarding to a UCD group. • A station is a member of a group call no answer. If the group is called, the call is not forwarded to the UCD group. Exception: The first subscriber entered has activated call forwarding to a UCD group. In this case, the call is forwarded.

15.6.1.1 How to Configure Call Distribution / UCD Groups

You can use the **UCD** wizard to configure intelligent call distribution to a group with selected stations.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **User Telephony**.

3) Click on **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.

4) To configure a UCD group, click **Edit** in the row containing the required UCD group.

5) Enter the call number of the new UCD group in the **Call number** field.

6) Enter the DID number of the new UCD group in the **Direct inward dialing number** field.

> **INFO:** If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

7) Enter the name of the UCD group in the **Name** field.
8) Click on **OK & Next**. The window **Assignment of UCD Agents** is displayed.
9) Mark the required UCD agent IDs in the **Selection** and assign them to this UCD group by clicking **Add**.
10) Click on **OK & Next**. The **Edit announcement/overflow** window appears.
11) Select the announcement of the UCD group in **Announcement** drop-down list. You can optionally select an announcement (if configured) or the internal Music On Hold (MOH). After you select the announcement, the **Ann. delay time** field appears.
12) In the field **Ann. delay time**, enter the time (in seconds) after which a caller in the queue is to receive an announcement.
13) Select the time after which a call is to be forwarded to the next UCD agent of the UCD group in the **Waiting time between agents** drop-down list.
14) Select the overflow destination for the UCD group in the **Overflow destination** drop-down list. You can select an external destination, another UCD group, an internal station or a group.

    If you select **External destination** as the overflow destination, the **External destination** field and the **Route** drop-down list appears.

    a) Enter the call number of the external overflow destination in the **External destination** field.
    b) If the external overflow destination is to be reached via a specific route, select the route in the **Route** drop-down list.
15) Click on **OK** to accept the entries.
16) If you want to configure further UCD groups, repeat steps 4 through 15.
17) Click on **OK & Next** followed by **Finish**.

15.6.2 UCD Agents

The stations of a UCD group (agents) comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. All incoming calls are distributed to the available stations in a UCD group.

The assignment of agents to the UCD groups occurs via identification codes (IDS). An ID can be assigned to no more than one UCD group. An agent can be assigned multiple IDs. This lets an agent work in more than once UCD group. An agent, however, can only be logged on and therefore active in one UCD group at a time.

In order to use the UCD functions effectively, agents should have phones equipped with a display, function keys and a headset.

Logging on/off

Agents can log into any phone of the communication system (except ISDN and SIP phones) by using their respective IDs (Identification Code). The agent is available following successful login and permanently assigned to the relevant phone until he or she logs off. The agent cannot log into another phone. Agents who have logged off are no longer considered for the call distribution.

The UCD functions for logging in, logging out and for changing the station status can be accessed by agents from the telephone via programmed function keys or via the associated menu items or via codes.

Subscriber states

An agent's state is **available** following successful login. If required, a agent can set his or her own station status, or the status may be changed automatically, depending on the agent's current activity. The current subscriber state is shown on the phone's display.

The following displays are possible:

Display	Meaning
available	The agent is available and can accept UCD calls.
not available	The agent temporarily logged off his or her workstation (for example, for a break).
wrap up	The agent is in wrap-up mode. He or she does not receive any UCD calls during the wrap-up time. Depending on the configuration, this can be an individual wrap-up time (the agent independently defines the length of the wrap-up time by changing his or her subscriber status) or an automatic wrap-up time (a wrap-up time is automatically available to all agents after a UCD call).
for <UCD group name>	The agent receives a UCD call.

An agent logs off after his or her shift and is therefore no longer available for UCD calls. The agent can still be reached at his or her personal station number.

If all agents of a UCD group are in the state **not available**, incoming calls are forwarded to an overflow destination (an external destination, another UCD group, an internal station or a group).

If an agent does not accept a call although he or she is logged on and available, the communication system automatically sets the status of that station to **not available**.

Dependencies

Topic	Dependency
Call forwarding	If an agent activates the Call Forwarding feature, he or she is automatically logged off and is no longer available for UCD calls.
ISDN phones, SIP phones	It is not possible to use ISDN and SIP phones here.

15.6.2.1 How to Add or Delete UCD Agents

The **UCD** wizard can be used to add UCD agents to a UCD group or to delete them from a UCD group.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.
4) To add UCD agents to a UCD group or delete them, click **Edit** in the row containing the required UCD group.
5) Click on **OK & Next** to go to the **Assignment of UCD agents** window.
6) Select one of the following options:
   - If you want to add a UCD agent, mark the required UCD agent IDs in the **Selection** and assign them to this UCD group by clicking **Add**.
   - If you want to delete UCD agents, mark the desired **Members** and delete them from the UCD group by clicking **Delete**.
7) Click on **OK & Next** to confirm the entries.
8) Click on **OK**.
9) If you want to edit the UCD agents of another UCD group, repeat steps 4 through 8.
10) Click on **OK & Next** followed by **Finish**.

15.6.3 Wrap up

This feature temporarily removes an agent from the call distribution in order to allow the agent some time to wrap up the call just completed. The agent does not receive any UCD calls during the wrap-up time.

A distinction is made between:

- the individual wrap-up time.

  The agent sets the wrap-up time length by changing his or her subscriber state.
- the automatic wrap-up time.

  The Uniform Call Distribution (UCD) feature is configured for this in such a way that a wrap-up time is automatically made available to all agents in all UCD groups after a UCD call. The automatic wrap-up time is defined in ring cycles, that is, in increments of five seconds.

  An agent can manually extend the automatic wrap-up time by changing his or her subscriber state.

An agent can be reached throughout the wrap-up time via his or her personal station number.

15.6.3.1 How to Change the Automatic Wrap-Up Time

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click on **Incoming Calls** > **UCD** in the menu tree.
4) Click on the **Edit UCD Parameters** tab.
5) Select the wrap-up time that should be available to all UCD agents in the **Wrapup Mode (Cycles)** drop-down list. This is defined in ring cycles, that is, in increments of five seconds.
6) Click on **Apply** followed by **OK**.

15.6.4 Call Prioritization

You can set a priority for incoming internal and external calls for a UCD group. The queued calls are distributed to the agents in a UCD group on the basis of priority and the wait time.

A queued call with a high priority is answered before a call that has been waiting longer but has a lower priority. A queued call with low priority will be forwarded to an overflow destination before a queued call with high priority.

Priorities are assigned on the basis of trunks for external calls (per B channel), regardless of whether IP or TDM lines are involved.

Examples:

- Communication system with ISDN Primary Rate Interface (S_{2M} interface) and ISDN Point-to-Multipoint connection (S_0 interface)

  Incoming calls via the ISDN Primary Rate Interface are normal customer calls. All B channels of the $_{2M}$ interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the S_0 interface are thus assigned a high priority.
- Communication system with a point-to-point connection to an Internet Telephony Service Provider ITSP and an ISDN point-to-multipoint connection (S_0 interface)

  Incoming calls via the PABX number for IP telephony are normal customer calls. All B channels of the LAN interface are thus assigned a medium priority. Calls received via the ISDN point-to-multipoint connection are urgent calls, e.g., high-priority orders for spare parts. All B channels of the S_0 interface are thus assigned a high priority.

The priority is set system-wide for internal calls and therefore applies equally to all internal calls.

Ten priority levels (1 = high, 10 = low) are available.

By default, priority = 10 is set for internal calls, and priority = 1 for external calls.

15.6.4.1 How to Change Request Priorities

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Click on **Incoming Calls** > **UCD** in the menu tree.
4) Click on the **Edit UCD Parameters** tab.
5) In the **Priorities, internal** drop-down list, select the priority that should apply to all internal calls for all UCD groups (1 = highest priority, 10 = lowest priority).
6) For each trunk (B channel), select the priority, in the associated **Priority** drop-down list, that is to apply to external calls over this trunk to all UCD groups (1 = highest priority, 10 = lowest priority). For every B channel, an individual priority can be set.
7) Click on **Apply** followed by **OK**.

15.6.5 Accepting UCD Calls Automatically

This feature lets agents accept incoming calls without any additional operations (Automatic Incoming Call Connection AICC).

This feature can only be used if the agent's phone has a headset and Disconnect key. An audible tone notifies the agent via the headset about an incoming call that is then automatically put through.

An agent can clear down an ongoing call by pressing the Disconnect key.

The "AICC" feature is not activated by default. Activation is performed on a group-specific basis and applies to all agents in a UCD group, irrespective of whether or not the agent's phone features a headset.

15.6.5.1 How to Change the Automatic Acceptance of UCD Calls

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **UCD** > **…** down to the desired UCD group.
4) Click on the **Edit UCD Groups** tab.

5) Select one of the following options:
   - If you want the UCD agents of this UCD group to be able to accept incoming calls without additional operating steps, select **yes** in the **AICC** drop-down list.
   - If you do not want the UCD agents of this UCD group to be able to accept incoming calls without the usual operating steps (such as picking up the handset, for example), then select **no** in the **AICC** drop-down list
6) Click on **Apply** followed by **OK**.

15.6.6 UCD queue

If all agents of a UCD group are busy, incoming calls can be placed in a queue. Announcements or music can be played for on-hold callers.

If a call that is waiting in the queue for a specific period (first call cycle) is not accepted by the agent longest in **available** state, this agent's state is changed to **not available** and the call is transferred to the next available agent. If this agent does not answer the call either within a set period (second call cycle), the status of this agent is changed to **not available**. The call is routed to the overflow destination if the status of all agents is **not available**.

For every UCD group, the maximum number of calls in the queue can be set individually. If the maximum number of waiting calls is exceeded, further calls can be routed to an overflow destination.

You can select an external destination, another UCD group, an internal station or a group as the overflow destination. If the overflow destination is another UCD group and if all other agents in this UCD group are busy, the call remains in the queue associated with the original group and is also entered in the queue of the other UCD group (overflow destination).

An agent can query the number of calls in the queue for his or her UCD group with a specially programmed function key of via the assigned menu item or code.

Calls in a Queue

The maximum number of calls in the queue is 30 for UCD groups 1 through 59 and 72 for UCD group 60.

The minimum number of calls in the queue is zero. There is no queue if the minimum number is set to zero. Calls are redirected or rejected directly at an overflow destination if there is no agent available.

15.6.6.1 How to Change the UCD Queue

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **UCD** > **…** down to the desired UCD group.

4) Click on the **Edit UCD Groups** tab.
5) Select the number of primary ring cycles in the **Prim. ring cycles** drop-down list. This is defined in ring cycles, that is, in increments of five seconds. This setting specifies how long a call remains in the queue if not accepted by the agent longest in "available" state. The call is then forwarded to the next available agent.
6) Select the number of secondary ring cycles in the **Sec. ring cycles** drop-down list. This is defined in ring cycles, that is, in increments of five seconds. This setting specifies how long a call remains in the queue if not accepted by the next available agent.
7) Select whether a change of announcement (Ann. change) should take place:
   - If the queued callers should hear the announcement only once, select the item **once** in the **Ann. change** drop-down list.
   - If the queued callers should hear cyclically varying announcements, select the item **cyclic** in the **Ann. change** drop-down list.
8) In the field **Ann. delay time**, enter the time after which a caller in the queue receives an announcement. The specification is made in seconds.
9) Click on **Apply** followed by **OK**.

15.6.7 UCD Overflow

UCD calls can be forwarded to an overflow destination if they are not accepted by the agents of a UCD group and if no queue was set up or if the maximum number of calls in the queue was reached.

NOTICE: The UCD overflow concept defines only one overflow destination, the second CDL entry. Therefore, the announcements are played only when the call is at the UCD overflow destination and not for the whole ringing cycle. When a call leaves the UCD overflow destination then default MOH is opened.

The maximum number of calls in the queue can be individually set for every UCD group. If this number is exceeded, further calls can be routed to an overflow destination.

If you do not want a queue to be created, you can enter zero as the maximum number of calls in the queue. Unanswered calls are then immediately routed to an overflow destination.

Dependencies

Topic	Dependency
AutoAttendant	It is not possible to use an AutoAttendant as an overflow destination.

15.6.7.1 How to Change the UCD Overflow

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Incoming Calls**.
3) Navigate in the menu tree under **Incoming Calls** > **UCD** > **…** down to the desired UCD group.
4) Click on the **Edit UCD Groups** tab.
5) Enter the maximum number of queued calls in the **Queued calls** field. Calls exceeding this number are redirected to an overflow destination.
6) Enter the desired time in the **Overflow time** field. The specification is made in seconds.

   Note: this setting is relevant only when an external UCD application is connected. If a queued call is not accepted by the UCD application within the overflow time, the call is processed further by the communication system in accordance with the Call Management specifications.
7) Click on **Apply** followed by **OK**.

15.6.8 UCD Night Service

An individual night service can be configured for every UCD group. Night service can also be activated and deactivated by every agent in a UCD group. Following activation, all calls for this UCD group are forwarded to the night destination.

The night service destination can be defined as an internal station, another group, an announcement/MoH, the voicemail box of the communication system or an external destination.

Activating / Deactivating

Activation or deactivation of the UCD night service can be achieved via a programmed function key or via the associated menu items or via codes. The call number of the desired night service destination must be entered at activation.

For more information on the communication system's night service, see Night Service .

Dependencies

Topic	Dependency
Subscriber state	If you activate the UCD night answer feature, your current subscriber status does not change. A forced logout of the agents who are still logged in does not occur.

Topic	Dependency
Communication system's night service	The communication system's UCD night answer and night service can be activated and deactivated independently of one another. Example: A UCD group was entered as the night service destination for the communication system. Calls that reach this UCD group via the communication system's night service remain in this UCD group, irrespective of a UCD night answer.
Existing calls	Existing calls are not affected by the activation of UCD night answer.

15.6.9 Announcements / Music on Hold for UCD

Music On Hold (MoH) or announcements can be played to callers who cannot be switched through directly to the agents of a UCD group. Music on hold and announcements can be assigned to each UCD group individually.

You have the following options:

- Music On Hold (MOH)

  Queued callers can be played music from the integrated source of the communication system. Further Music on Hold file(s) can be loaded from a PC into the communication system.

  For more information, see Music on Hold
- Announcements

  Queued callers can be played integrated announcements. Further announcements can be loaded from a PC into the communication system.

  For more information, see Announcements

The time up to the start of the announcement can be set (**Ann. delay time**). You can suppress the announcement by setting the maximum value (600 seconds). It is assumed here that the call will be accepted within this time.

15.6.9.1 How to Change Announcements / Music on Hold for UCD

You can use the **UCD** wizard to configure announcements and/or Music on Hold for UCD groups.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.
4) To change the announcements / music on hold for a UCD group, click **Edit** in the row containing the required UCD group.

5) Click **OK & Next** until the **Edit announcement/overflow** window appears.
6) Select the announcement of the UCD group in **Announcement** drop-down list. You can optionally select an announcement (if configured) or the internal Music On Hold (MOH). After you select the announcement, the **Ann. delay time** field appears.
7) In the field **Ann. delay time**, enter the time (in seconds) after which a caller in the queue is to receive an announcement.
8) Click on **OK** to accept the entries.
9) If you want to add announcements / Music on Hold to another UCD group, repeat steps 4 through 8.
10) Click on **OK & Next** followed by **Finish**.

15.6.10 Transfer to UCD Groups

Internal and external calls can be transferred to UCD groups. If a call is not answered within a certain period, a recall is carried out.

The recall time is defined via the time parameter **Monitoring transfer to a UCD group prior to answer**. The default setting is 300 seconds. This setting can be changed by an administrator with the **Expert** profile in **Expert mode**.

Dependencies

Topic	Dependency
Announcements	Announcements can be played for the external transferred calls. This is not possible for internal calls.
Recall time	The recall time for a transfer to UCD groups differs from the recall time for transfers to other subscribers.

15.6.10.1 How to Edit the Recall Time for Calls Transferred to UCD Groups

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **Time Parameters**.
4) Enter the desired recall time for the time parameter **Monitoring transfer to a UCD group prior to answer** (default setting = 300 seconds). If a call is not answered before this period expires, a recall occurs
   a) Select the desired time base in the **Base** drop-down list.
   b) In the **Factor** field, enter the value with which the time base is to be multiplied.
5) Click on **Apply** followed by **OK**.

15.6.11 Releasing UCD from Analog Lines

When UCD calls over analog lines are not answered within a specific time, these calls are released. This prevents analog lines from freezing up.

The release time is defined via the time parameter **Monitoring a UCD call on an analog line**. The default setting is 300 seconds. This setting (from 0 to 255 minutes) can be changed by an administrator with the **Expert** profile in **Expert mode**.

15.6.11.1 How to Edit the Release Time for UCD Calls over Analog Trunks

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **Time Parameters**.
4) Enter the desired release time for the time parameter **Monitoring a UCD call to an analog line** (settable from 0 to 255 minutes; default setting = 300 seconds). Calls that are not answered before this time expires are released.
   a) Select the desired time base in the **Base** drop-down list.
   b) In the **Factor** field, enter the value with which the time base is to be multiplied.
5) Click on **Apply** followed by **OK**.

16 Call Routing

The communication system provides several ways to assign calls to a desired destination, such as classes of service (toll restriction), day and night service, least cost routing and Call Admission Control (CAC). Emergency calls can be made from any configuration.

16.1 Classes of Service (Toll Restriction)

Classes of service (Toll restriction) control subscriber access to external lines that may be subject to toll charges.

Related concepts

Configuring Stations on page 429

16.1.1 Class of Service (COS) Groups and Classes of Service

Every subscriber is assigned a Class of Service group that defines the class of service (i.e., the permissions) of the subscriber for incoming and outgoing calls.

For each route, one of the following classes of service is defined in the COS group:

- **Internal**

  The subscriber may only make internal calls.
- **Outward-restricted**

  The subscriber may only answer (not make) external calls.
- **Allowed list** 1-6

  The subscriber may only dial the external numbers defined in the Allowed list. Outward-restricted trunk access applies if no call number is entered.
- **Denied list** 1-6

  The subscriber is not permitted to dial the external numbers defined in the Denied list. Unrestricted trunk access applies if no call number is entered.
- **Unrestricted**

  Subscribers can answer and set up incoming and outgoing external calls without restriction.

Some of the 15 possible COS groups are preset with the same class of service for all routes and given meaningful names (e.g., COS group **International** with the class of service **Unrestricted** or COS group **Incoming** with the class of service **Outward-restricted**). The names of all COS groups can be changed by the administrator.

NOTICE: By default every station belongs to COS group 7 and this can be changed. Also every trunk belongs to COS group 7 but this is not configurable so as a result COS group 7 should not be used and let it have Unrestricted access to every Trunk Group.

Dependencies

Topic	Dependency
Speed Dials	System speed dial destinations can be selected independently of the assigned COS group.
LCR	The Class of Service Groups (Toll Restriction) and LCR Class of Service are different.
Call forwarding	For forwarded calls, the caller's class of service applies.

16.1.1.1 How to Edit COS Group Names

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click on **Day: Class of Service Group** in the menu tree.

NOTICE: You can also click in the menu tree on **Night: COS group** to achieve the same result.

---

4) Click on the desired COS group in the menu tree.
5) Click on the **Edit COS Group** tab.
6) Enter the name of the COS group in the **Class of Service Group** field.
7) Click on **Apply**, followed by **OK**.

16.1.1.2 How to Edit the Classes of Service of a COS Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click on **Day: Class of Service Group** in the menu tree.
4) Click on the desired COS group in the menu tree.
5) Click on the **Edit COS Group** tab.
6) Select to desired class of service for the Day mode for each route being used from the drop-down list.
7) If required, select the **Networking** class of service for the Day mode.
8) Click on **Night: Class of Service Group** in the menu tree.
9) In the menu tree, click on the COS group you have just edited.
10) Click on the **Edit COS Group** tab.

11) Now select the desired class of service for the Night mode for each route being used from the drop-down list.
12) If required, select the **Networking** class of service for the Night mode.
13) Click on **Apply**, followed by **OK**.

16.1.1.3 How to Display All Stations of a COS Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click on **Day: Class of Service Group** in the menu tree.

NOTICE: You can also click in the menu tree on **Night: COS group** to achieve the same result.

---

4) Click on the desired COS group in the menu tree.
5) Click on the **Display COS Member** tab. All subscribers to whom the selected COS group is assigned are displayed with their respective call numbers and names.

16.1.2 Allowed and Denied Lists

Allowed and Denied lists are used to define which external phone numbers may and may not be dialed by the subscribers.

Allowed lists contain the digit strings permitted at the start of a phone number. The subscriber may only dial the external numbers defined in the Allowed list. Make sure that all required emergency numbers are also included in the list!

Denied lists contain the digit strings that are not allowed at the start of a phone number. The subscriber is not permitted to dial the external numbers defined in the Denied list. Make sure that no emergency numbers are included in the list!

The **List of Emergency Numbers** is a special case of the Allowed list. The subscriber may only dial the emergency numbers entered in the list. Make sure that all required emergency numbers are included in the list!

It is not necessary to enter the complete phone numbers in the lists. To permit users to dial (toll free) 0800xxx numbers, for example, only `0800` needs to be entered here. Since these lists are only for outgoing external calls, it is not necessary to include the CO access code with the numbers you enter. Entering a `#` sign at the start of a denied number prevents the toll restriction from being bypassed for system telephones when an analog CO line is to be seized using DTMF signaling or when switching to DTMF during the dialing.

The Administrator can use **exception filters** for any Denied list to define which digits should not be compared with the corresponding Denied list. The communication system excludes the set range of digits before the digit analysis. By prohibiting the characters `*` and `#`, subscribers are prevented from entering these characters to bypass the toll restriction.

Configuration Limits

Feature	Number
Allowed list 1: long, 100 entries	1
Allowed lists 2-6: short, 10 entries	5
Denied list: long, 50 entries	1
Denied lists 2-6: short, 10 entries	5
Number of characters in list entries (digits 0 - 9 and the characters * and #)	26

16.1.2.1 How to Create a List of Emergency Numbers

You can create a list of emergency numbers for the "Emergency Numbers" COS group with the **Class of Service** wizard.

Prerequisites

You are logged in at the WBM.

Your communication system is connected to a trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Classes of Service** wizard.
4) Enter an emergency phone number in the input field and click on **Add**. The phone number is added to the list of emergency numbers.
5) If you want to enter more numbers into the list of emergency numbers, repeat the previous step.
6) Keep clicking on **OK & Next** until you complete the configuration with **Finish**.

16.1.2.2 How to Create an Allowed and a Denied List

You can create an Allowed and a Denied list with the **Class of Service** wizard.

Prerequisites

You are logged in at the WBM.

Your communication system is connected to a trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Classes of Service** wizard.
4) Click on **OK & Next**.
5) Enter an allowed phone number without the CO access code in the input field and click on **Add**. The phone number is added to the Allowed list.

6) If you want to enter more numbers into the Allowed list, repeat the previous step.
7) Click on **OK & Next**.
8) Enter an denied phone number without the CO access code in the input field and click on **Add**. The phone number is added to the Denied list.
9) If you want to enter more numbers into the Denied list, repeat the previous step.
10) Keep clicking on **OK & Next** until you complete the configuration with **Finish**.

16.1.2.3 How to Create Additional Allowed Lists

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Allowed Lists** in the menu tree.
4) Click on the desired allowed list in the menu tree.
5) Click on the **Add Station Number** tab.
6) Enter the external **Call number** without the seizure code.
7) Click on **Apply**, followed by **OK**.
8) If you want to add more call numbers, repeat steps 6 and 7.
9) If you want to create additional allowed lists, repeat steps 4 through 7.
10) You can view all the phone numbers of the selected Allowed list on the **Display List** tab.

16.1.2.4 How to Create Additional Denied Lists

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Denied Lists** in the menu tree.
4) Click on the desired denied list in the menu tree.
5) Click on the **Add Station Number** tab.
6) Enter the external **Call number** without the seizure code.
7) Click on **Apply**, followed by **OK**.
8) If you want to add more call numbers, repeat steps 6 and 7.
9) If you want to create additional denied lists, repeat steps 4 through 7.
10) You can view all the phone numbers of the selected Denied list on the **Display List** tab.

16.1.2.5 How to Display all Call Numbers in a Denied List

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Denied Lists** in the menu tree.
4) Click the desired number on the Denied List in the menu tree.

16.1.2.6 How to Display all Call Numbers in an Allowed List

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Allowed Lists** in the menu tree.
4) Click on the desired number on the Allowed List in the menu tree.

16.1.2.7 How to Edit the Analysis Filter for the Denied List

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Denied Lists** in the menu tree.
4) Click the desired number on the Denied List in the menu tree.
5) Click on the **Edit Analysis Filter** tab.
6) Select a range in the **From digit** and **To digit** drop-down lists.

   This enables a range within a call number to be configured. The starting position of the range is selected via the **From digit** drop-down list and the end position via **To digit**. .

   The default setting of ***** and **#** for this field is intended as a means of blocking these characters, since * and # could be used as "dummy" characters, which are not evaluated in the Central Office and would thus bypass the toll restriction. Entering * and # in the Denied list causes these characters have no effect, so only the dialed digits are evaluated.
7) Enter the character(s) to be hidden in the **Character** field.
8) Click on **Apply** followed by **OK**.

16.1.3 Blacklist

A blacklist is available within the OpenScape Business system that allows blocking of incoming calls from specific caller numbers (CLI) and from calls without caller number or restricted presentation of caller number.

The blacklist supports up to 100 numbers with max 25 digits either in canonical format (e.g., +4989) or in international format (e.g., 004989). Supported characters are 0-9 digits and the '+' character. The '+' character refers to the international prefix that is configured in the system. It has to be entered always at the first position. Number fragments starting from the beginning of the caller number (CLI) are allowed. A logical check is performed during the entry of a number into the blacklist. The number is refused if it has already been entered or if it is covered by a number fragment.

Check of transmitted caller numbers is always done using the international format. Caller numbers are converted into the international format according to the route data, if they are transmitted in other formats.

The blacklist is applied to all Central Office trunks that are configured in the system. It supports multiple Central Office/ Telephony Providers with different country / local area codes.

An event log entry is created by the blacklist for each blocked call.

Within an OpenScape Business network, the blacklist needs to be configured in every node that is connected to Central Office / Telephony Providers, respectively in the gateways. Network internal calls are not restricted by the blacklist.

The blacklist can be enabled / disabled by the system administrator. In addition, a separated flag can be set for the blocking of anonymous calls.

Service log logs contain information about blocked called numbers. Log entries that correspond to blocked called numbers contain the EventText **!BlackListed Call:**. To find the called number that was blocked, you need to check the last two digits of the log entry. These digits (in hexademical form) correspond to the position in the blacklist that contains the blocked number. If these digits are ff, then the blocked call is anonymous.

Dependencies

Calls with CLI suppression are not blocked as anonymous calls by the system in case that the flag **Call number suppression override** is set within the system. The caller number has to be entered explicitly in the blacklist in this case. The flag **Call number suppression override** is disabled in factory default settings. It can only be enabled using the Manager E.

The mobility feature of the system can be affected by the blacklist if mobile numbers of Mobility Users are entered in the blacklist. In this case the call to the DISA port in Call Through mode is blocked by the blacklist.

16.1.3.1 How to Create a Blacklist for incoming calls in Expert mode

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click on **Telephony Server > Classes of Service.**
3) Click **Classes of Service > Blacklist** in the menu tree.
4) Click on the **Add Call Number** tab.
5) Enter the **Call number**.
6) Click on **Apply**, followed by **OK**.
7) If you want to add more call numbers, repeat steps 5 and 6.
8) The added call numbers of the Blacklist are displayed on the **Display list** tab under **Blacklist** area or under **Blacklist** in the menu tree.

   The system administrator should be able to block unwanted callers permanently.

   - Enable the check box **Block Anonymous calls** in Anonymous calls area in order to block an anonymous incoming call.

     NOTICE: Anonymous calls are defined as the calls for which the originator number will not be displayed to the user.

   - Enable the check box **Blacklist feature on** in Blacklist area in order to block specific call numbers.

     NOTICE: Blacklist feature is based only on calling party number (call originator) given by the provider.

16.1.3.2 How to Edit/Delete Call Numbers in the Blacklist

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click **Telephony Server > Classes of Service.**
3) Click **Classes of Service > Blacklist** in the menu tree.
4) Click on the desired number on the Blacklist in the menu tree.
5) The administrator can edit or delete the selected entry.

   In order to edit the selected entry:

   - Click on the **Edit Station Number** tab.
   - Enter the desired call number in the **Call Number** field.
   - Click on **Apply** followed by OK.

   In order to delete the selected entry:

   - Click on the **Delete Call Number** tab.
   - Enter the desired call number in the **Call Number** field.
   - Click on **Apply** followed by OK.

6) The system administrator should be able to block unwanted callers permanently.
   - Enable the check box **Block Anonymous calls** in **Anonymous calls** area in order to block an anonymous incoming call

     NOTICE: Anonymous calls are defined as the calls for which the originator number will not be displayed to the user.

   - Enable the check box **Blacklist feature on** in **Blacklist** area in order to block specific call numbers.

     NOTICE: Blacklist feature is based only on calling party number (call originator) given by the provider.

16.1.3.3 How to Display Call Numbers in the Blacklist

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click **Telephony Server > Classes of Service.**
3) Click **Classes of Service > Blacklist** in the menu tree.
4) Call numbers are displayed under **Blacklist** in the menu tree or in the **Display List** tab under **Blacklist** area.

16.1.3.4 How to Create a Blacklist for incoming calls in Setup

You can create a Blacklist with the **Blacklist for incoming calls** wizard.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Blacklist for incoming calls** wizard.
4) Enter an allowed call number in the input field and click on **Add**. The call number is added to the Blacklist.
5) Click on OK & Next.
6) If you want to enter more numbers into the Blacklist, repeat the steps 4 and 5.
7) If you want to delete a call number, click on **Delete**.
8) Keep clicking on **OK & Next** until you complete the configuration with **Finish**.

16.1.4 Night Service

During the night, incoming and outgoing calls can be treated differently than during the day. Incoming calls can be redirected to a night service destination, and internal subscribers can have different classes of service for their phones than during the day. The system-wide switching between the day and night service is performed automatically at a time specified by the administrator.

Scheduled Night Service

Variable Night Service

Any phone can serve as a night service destination, provided the associated class of service group allows incoming calls. A telephone with internal authorization only cannot be entered as a night service destination. If the night service destination has activated call forwarding, this is followed.

In order to prevent toll fraud, for example, a COS group can be assigned different classes of service for the night and day modes.

In addition, you can also specify a different intercept position for the night service as opposed to the day service. This intercept position can be an individual station or a group.

The communication system activates and deactivates the night service in accordance with a schedule defined by the administrator.

INFO: With the scheduled night service, the active settings apply to ALL stations of the communication system. In the case of automatic COS changeover after time, all subscribers are combined into groups (profiles).

The variable night service is activated and deactivated manually by an authorized subscriber. The calls are handled as configured by the administrator in the call destination lists

By default, the first subscriber (with the station number "100") in the communication system can activate and deactivate the night service. The administrator can authorize up to five subscribers to activate and deactivate the night service.

UCD Night Service

An individual night service can be configured for every UCD group. It can be activated and deactivated independently of the system-wide night service. It can also be activated and deactivated by every agent in a UCD group. The current status of the individual agents and existing calls are not affected. Following activation, all calls for this UCD group are forwarded to the night service destination.

Another UCD group, an internal station or an external destination can all be set as a night service destination.

16.1.4.1 How to Assign Classes of Service for the (Manual) Night Service

You can use the **Classes of Service** wizard to assign individual subscribers the authorization to switch the communication system from the day to night service (and vice versa) via their telephones. The switch between day and night service occurs via the telephone by using a code.

Prerequisites

You are logged in at the WBM. Your communication system is connected to a trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Classes of Service** wizard.
4) Click on **OK & Next** until you see the **Authorized station for night service** window.
5) Mark the desired station in the list under **Stations** and click **Add**. The station will then appear in the list under **Authorized station**.
6) Click on **OK & Next**.
7) A list of all authorizations (classes of service) appears in the **System Overview** window.
8) Click on **Finish**.

16.1.4.2 How to Delete Classes of Service for the Manual Night Service

The **Classes of Service** wizard can be used to delete the authorization of a station to switch from the day to night service.

Prerequisites

You are logged in at the WBM. Your communication system is connected to a trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Classes of Service** wizard.
4) Click on **OK & Next** until you see the **Authorized station for night service** window.
5) Mark the desired station (whose class of service you want to delete) in the list under **Authorized station** and click **Delete**.
6) Click on **OK & Next**.
7) A list of all authorizations (classes of service) appears in the **System Overview** window.
8) Click on **Finish**.

16.1.4.3 How to Configure the Scheduled Night Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click in the menu tree on **Autom. night service** > **Monday** (Monday is just an example; all days of the week are available).
4) Under **Edit Zone**, select one of four possible zones to which a specific Class of Service should apply.
5) Specify the time (in hours and minutes) for this class of service with **Start** and **End**.
6) Under **Night Call no.**, select the authorized subscriber.

   Your settings for each zone will be displayed in the **Autom. night service** field.
7) Click on **Apply** followed by **OK**.
   When night service is active, a message **The system is currently running in night mode** is displayed on the Admin Portal landing page.

16.1.4.4 How to Configure a Special Day for the Scheduled Night Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **Special Days** in the menu tree.
4) Select the year for which you want to define a holiday by using **>>** or **<<**.
5) Then use **>>** or **<<** to select the month fort that holiday.
6) Then click in the calendar on the day to be defined as a holiday.
7) Enter a designation for the holiday under **Name**.
8) Click on **Apply** followed by **OK**.

16.1.4.5 How to Delete a Special Day for the Scheduled Night Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.

3) Click **Classes of Service** > **Autom. night service** > **Special Days** in the menu tree.
4) Under **Day**, click on the trash can to the left of the holiday to be deleted.
5) Click on **Apply**, followed by **OK**.

16.1.5 Automatic COS Changeover after Time

For the "automatic COS changeover after time", the stations are grouped into so-called station profiles that define which COS group applies in which time interval of the week. For each station profile, you can configure a schedule.

Dependencies

Differences between "automatic COS changeover after time" and the "scheduled night service":

- Automatic COS changeover after time applies only to the day service (not the night service).
- Reaching the call destination via Call Management

  This takes place via Call Management and does not depend on automatic class-of-service changeover. There are different call lists for day and night.
- With the scheduled night service, a distinction can only be made between day and night shifts, and this applies to ALL stations.
- Intercept destinations

  The intercept destination is only defined by the scheduled night service.
- COS group:

  During the night, the COS group is in a constant (configurable) relationship with the station; the automatic class of service changeover after a timeout has no impact on this.

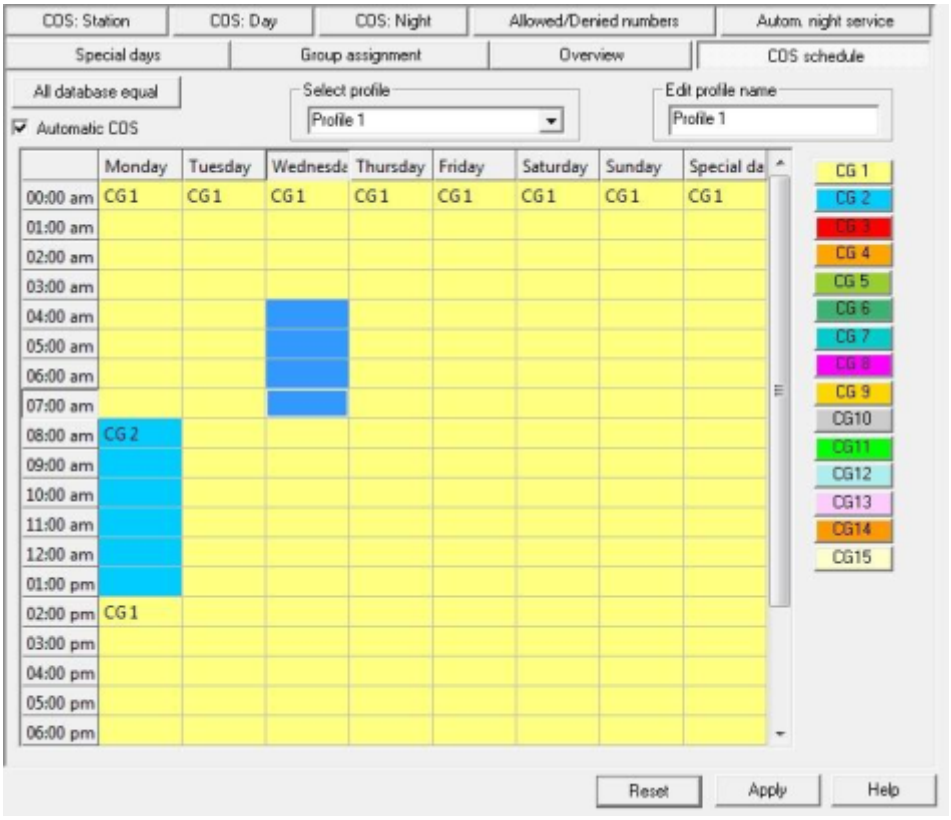
  During the day, the COS group may be changed during certain times of the day or also be in a fixed (configurable) relationship with the subscriber.

Topic	Dependencies
Night service	The "Automatic Night Service" feature has priority over the "Automatic COS Changeover after Time" feature. If the night service is activated, the COS group is handled normally and applied for the night. The schedule is only relevant during the day.
Networking	Automatic COS changeover and night service do not function across all nodes.

16.1.5.1 Schedule

The schedule is used to control the Classes of Service for the "automatic COS changeover after time". It is possible to configure up to eight COS changeovers per day for each day of the week.

Each day begins at 00:00 hours. Entering the end time time in each of the columns delineates the time zones. In the following example of a schedule, the individual COS changeovers are referred to as CG2, CG4 and CG5.



A station can have different class of service groups for the day and night.

If "Automatic COS changeover" is set system-wide for the day, the profile and schedule that is configured will determine the COS group that is assigned to a station. At night, the station has the same COS group as previously assigned (via the night service).

Automatic COS changeover after time is disabled by default

The communication system supports only one time zone (world time). Remote station groups working in different time zones are set to the communication system's time zone.

The schedule can only be configured using Manager E.

16.1.6 CON Groups

The CON Groups feature is used to define which subscribers of the communication system can establish connections to which other subscribers of the communication system. This feature is used for tenant systems, for example.

CON groups can also be used to configure which lines individual subscribers can access for incoming and outgoing calls..

The CON functionality does not access the applications; it is only significant for telephony. The presentation of the presence status, for example, is not prevented by an access restriction through CON.

The CON feature is implemented in two steps:

- Create CON groups

- Configure CON matrix

INFO: The CON feature should not be used in conjunction with UC functionality, since this could result in limitations.

16.1.6.1 CON groups (traffic restriction groups)

CON groups (also referred to as traffic restriction groups) control allowed and denied connections between subscribers and lines of the communication system.

Using CON groups, specific stations and lines can be combined into groups.

You can assign a CON group to individual stations and lines in the communication system via the CON Group Assignment. When coding the connection matrix, you can then access these groups and define which subscribers can reach which other subscribers and which lines can be accessed by them.

All stations and CO trunks are assigned to CON group 1 by default. This provides all subscribers with unrestricted access to other subscribers as well as trunks, both incoming and outgoing. The CON matrix specifies which of the six CON groups can set up connections to which other CON groups.

A maximum of 64 CON groups can be configured.

NOTICE: CON group rules do not apply to SIP phones when a conference is initiated from a SIP phone between two restricted trunks.

16.1.6.2 Assigning Speed-Dialing Numbers to CON groups

Every CON group is assigned a range of System Speed Dialing (SSD) destinations. When a subscriber dials an SSD, the associated CON group is checked to verify if the subscriber is authorized to do so. Dialing is performed if this speed-dialing number lies within the correct range for the relevant CON group, otherwise an error message is output.

When a user dials a speed-dial number, the system identifies the ITR group for the number, which determines whether or not the user is authorized to dial that number. If not, an error message appears, and the dialing attempt is rejected

Speed-dial number ranges can overlap in the ITR groups.

By default, all speed-dial numbers are assigned to ITR group 1.

The speed-dial number ranges can overlap in the CON group. The following are permitted, for example:

CON group	SSD range
1	0000-7999
2	0050-0150
3	0200-0500

Please note, however, that you cannot enter individual system speed-dial (SSD) numbers or multiple SSD ranges in a CON group instead of a range. The following are not permitted, for example:

CON group	SSD range
1	0000, 0005, 0010
2	0050-0100, 0300-0500

16.1.6.3 How to Assign Stations to a CON Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **CON Group Assignment** > **CON Group Assignment** in the menu tree.
4) Select the entry with the desired traffic restriction group for one of the stations displayed in the **Stations** column in the **Group** drop-down list.
5) Click on **Apply**, followed by **OK**.

16.1.6.4 How to Assign a Trunk to a CON Group

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click **Classes of Service** > **CON Group Assignment** > **Trunk to CON Group** in the menu tree.
4) Select the entry with the desired traffic restriction group for one of the trunks displayed in the **Trunks** column in the **Group** drop-down list.
5) Click on **Apply**, followed by **OK**.

16.1.6.5 How to Edit the CON Matrix

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Classes of Service**.
3) Click on **Classes of Service** > **CON Matrix** in the menu tree.

4) Edit the connection options as follows:

- If you want to block all connection methods, click **Block all**.
- If you want to release all connection methods, click **Release all**.
- If you want to release only the group-internal connection methods, click **Group-internal only**.
- If you want to selectively edit one connection method between two CON groups, click in the field at the intersection point of these CON groups in the CON matrix. Click repeatedly in the field to release or block the connection methods in one direction, the other direction, or both directions.

5) Click on **Apply** followed by **OK**.

16.1.7 System Telephone Lock (COS Changeover)

The central lock code enables an authorized subscriber (possibly the administrator) to set a comprehensive lock on most of the phone functions for other subscribers. Only the following features are still available: internal calls, system speed dialing and conferencing with internal subscribers. This lock code can be deactivated by either the authorized subscriber or the locked subscriber by entering their own lock codes.

The lock code of the phone for the which the lock is to be activated or deactivated by the authorized subscriber is not required to set the lock.

By default, the authorized subscriber is the subscriber with the call number "100" (reconfigured).

16.1.8 Individual Lock Code (Locking the Phone)

If the individual telephone lock is set for a phone, external calls cannot be conducted from that phone, and the user settings cannot be modified.

Emergency numbers can be dialed even if the phone is locked.

You can still conduct internal calls.

Incoming calls can be redirected to internal subscribers.

A locked telephone only supports features that do not require external dialing. The System Speed Dialing feature is the exception to this rule.

To remind subscribers that the station is locked, the phone receives a steady tone (special dial tone). In addition, on phones equipped with a display, the message "Unlock Phone" appears.

Subscribers can lock their phones via a key or code by entering their personal lock codes and then unlock the phone again as required.

The phone lock code must be configured first before the phone lock can be used. The phone lock code is set to 00000 by default for all phones and can be set individually. To do this, the must be unlocked. The phone lock code must always be 5 digits. Only digits 0-9 are allowed. If the subscriber has forgotten the phone lock code, he or she can have it reset to the default value 00000 by an authorized user (i.e., the first station in the system with the call number "100" or the administrator).

16.1.8.1 How to Reset the Individual Lock Code

Use the **Station name and release** wizard to reset the individual lock code on a phone.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Station Name and Release** wizard. The **Name Configuration and Unlock for Stations and Groups** window appears.
4) Enable the check box **System telephone lock reset**.
5) Click **OK & Next** followed by **Finish**.

16.1.9 Collect Call Barring per Trunk (for Brazil only)

Collect call barring per trunk provides for automatic release of incoming collect calls. This feature is available only in the country settings for Brazil. The setting is ignored in all other countries.

Users can configure it individually for each analog trunk. Ringback protection can be configured individually for each analog trunk. If this feature is enabled for a trunk, the system opens the loop for two seconds (default value) one second (default value) after an incoming call is accepted. This ensures that collect calls are released in the network, while other calls continue unaffected.

16.1.10 Ringback Protection per Station (for Brazil only)

Ringback protection per station (also called call collect barring per station) makes it possible to set up ringback protection individually for each station, thus making it possible to automatically refuse incoming ringback calls. This also applies in the case of call forwarding, call pickup, an intercept, etc.

Users can also program collect call barring system-wide. This applies if a caller dials a hunt group instead of an individual station or misdials a number.

16.2 LCR (Least Cost Routing)

The Least Cost Routing (LCR) function automatically controls the paths used for routing an outgoing connection. This path can be routed via the public network, various network providers (ITSPs) or a private network. The most suitable connection path is selected for a call on the basis of the dial plan, route tables, and outdial rules.

Connections can be voice calls, analog data connections via fax and modem and ISDN data connections.

16.2.1 LCR Functionality

You can use the LCR function to specify the provider you want to use, for example, for local calls, mobile phone calls or international calls. You use the communication system to define the least-cost provider and conduct all calls via this specific path.

If a pattern that matches the dialed phone number is found in the dial plan, the route tables are searched for a suitable route (Each trunk is assigned to a route. See CO Access over Digital and Analog Lines). At the same time, the system checks if the LCR class of service applies to this route table entry. The LCR class of service and the difference between LCR and doll restriction are described in LCR Class of Service section.

The LCR function provides control over which stations of the communication system may use which routes or trunks (to ensure that faxes are routed exclusively via TDM trunks and not via ITSPs, for instance). It is also checked whether the caller has the required class of service as per the toll restriction to seize the route under consideration by LCR. This check can be disabled for tie trunks (PABX trunks) via the configuration.

The dialed digits are buffered until the routing tables with the LCR classes of service have been evaluated. It is only on completing this step that the connection is set up, in accordance with the outdial rules. A dial tone can be issued to signal the ready-to-dial condition to the subscriber.

When configuring outdial rules, you can enter information for the dialing station, e.g., by specifying that this connection is routed via a specific telephony provider (name of the provider) or that a connection is using a more expensive route. This information can either be displayed on the screen, output as a tone or output both on the display and as a tone.

In general:

- When LCR is activated, the check is performed for every external dialing operation. Exception: when dialing a specific trunk code or line key.
- If LCR determines that the preferred route cannot be used, the communication system will look for a (possibly more expensive) alternative from the routing table.
- Digits can be transmitted either individually or en-bloc, depending on the access method and the route table.
- If the table of DID numbers is empty, the table of internal call numbers is alternatively used. The corresponding rules apply to this table.

INFO: The location number (country code / possibly local area code / possibly PABX number) must be configured even for communication systems with analog trunks (MSI).

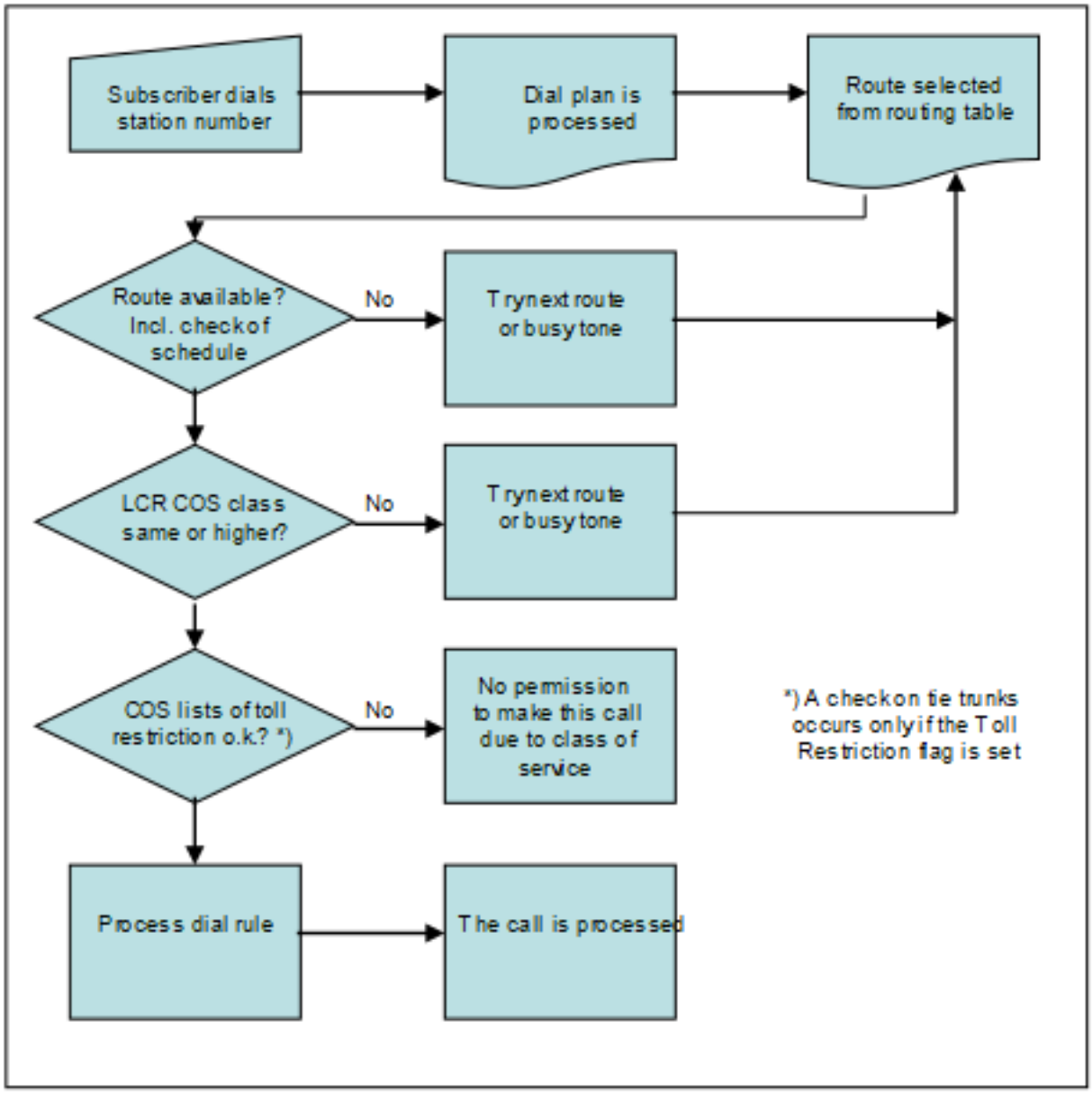
In addition, a DID number or, if the DID number table is empty, a DID number of the own analog trunk connection (MSI) must be configured. This is the only way to ensure that all external destinations can be reached.

System-Specific Information

The communication system evaluates a total of 24 characters.

The communication system can manage up to 1000 dial plans and 254 route tables with 16 entries each.

LCR Flowchart



Digit transmission

There are two types of digit transmission: digit-by-digit and en-bloc sending. For digit-by-digit transmissions, each digit is transmitted and processed directly after dialing (prerequisites: the LCR analysis is complete, the dial plan entry is uniquely identified, and the classes of service have been checked). With block dialing, digit blocks are formed and transmitted as a block (i.e., line seizure occurs only after some time or when an explicit end-of-dialing code is recognized).

The digit transmission for ITSP routes must always be en-bloc. The setting of the route apples to the entire routing table.

For U.S. only: Carrier Select Override

Carrier Select Override can be implemented through selective line seizure (code, key). The LCR mechanism is bypassed completely in this case.

Dependencies

Topic	Dependency
Schedule	If an LCR configuration with a schedule exists in a system migrated from HiPath 3000, these entries are still effective and can be administered with Manager E.
System Speed Dialing	To ensure that system speed dial destinations work properly, the LCR access code, followed by the destination number, must be entered in the speed-dial destination.
Name keys	Repertory dial keys to external destinations must have the LCR access code for proper operation.
Class of service (Toll restriction)	The toll restriction classes of service are also applied in LCR. For PBX trunks, the toll restriction can be disabled; the configuration occurs via a flag.
Prime Line	If Prime Line to the CO is used, no LCR is possible. These features are not mutually compatible.

16.2.1.1 How to Release LCR

Prerequisites

You are logged into the WBM with the **Expert** profile.

INFO: Some entries such as the local area code or station numbers will have already been created in the **Basic Installation** wizard. Manual changes to these entries should only be made by trained technician. An invalid configuration in the LCR could potentially prevent or restrict outgoing connections.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **LCR**.
3) Click on the **LCR Flags** tab.
4) Select the **Activate LCR** check box.
5) Click on **Apply** followed by **OK**.

16.2.2 LCR Dial Plan

The dial plan is searched for patterns that match the dialed digits (dialing sequence). The result is used as a criterion for selecting the route table. At the same time, the system checks if the subscriber's LCR class of service matches for this dial plan entry.

The pattern of a dialing sequence is assigned in the dial plan to a routing table which, in turn, determines further parameters for the connection setup.

The dial plan is split into individual fields for identification and configuration purposes. The table shows the numbers 4922000 and 1603656260 entered in the dial-plan table.

Field 1		Field 2		Field 3		Field 4		Field 5
0	C	492	–	2000				
0	C	160	–	365	–	62	–	60

The following entries apply for the phone numbers:

0 . . . 9	Allowed digits
–	Field separator
C	Simulated dial tone (can be entered up to three times). This entry is also interpreted as a field separator
Global character	
X	Any digit from 0 to . . 9
N	Any digit from 2 to . . 9
Z	One or more digits to follow up to the end of dialing

A digit sequence can be divided into a maximum of 10 fields.

Field separators are used to split the digit string into individual fields that can be evaluated separately. Example: After the first dialed digit, a separator is inserted so that a dialed “0” is detected as a separate field and thus simulates toll restriction.

Due to this field separation, these fields can be repeated or rearranged in the dial plan. The fields formed by the field separators "–" and "C" in the dial plan can be addressed selectively to repeat, suppress, exchange, or insert digits.

A "#" or "*" character in the digit string dialed by the subscriber is the end-of-dial code or indicates dialing method changeover. This is why these characters are not valid entries in the dial plan.

Specific dialed numbers must precede wildcard entries to prevent conflicts in matches with wildcard entries.

The account code entry can be enforced per dial plan. The Account Code Checking Procedure applies.

If there are multiple dial plan entries that match a a dial string, the closest match is used. Example: If 00894711 is dialed, and dial plan entries 0CZ and 0C089Z exist -> 0C089Z will be executed. The position of the entries within the dial plan is irrelevant; no "sorted" entry is required.

OpenScape Business can evaluate a dialing sequence of up to 24 characters.

LCR Entries for Initial Setup of the Communication System

When the communication system is started up for the first time, a number of country-specific default values are entered in the LCR dial plan. Up to and including dial plan 34, system-side entries for emergency calls, directory assistance, special numbers, default trunk seizure for PSTN and ITSP, for UC Suite, announcement connections, networking and for international dialing formats are preset to ISDN trunks. This range can be affected by configuration changes elsewhere (for example, by changes to the **Location number** flag). Consequently, whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected (which is important when dialing public numbers).

INFO: From LCR dial plan 36 onwards, all entries are freely available.

16.2.2.1 How to Edit the Dial Plan

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan**.
4) The individual dial plans are listed under **Change Dial Plan** and you can edit the following fields:
   - **Name**
   - **Dialed digits**
   - **Route table**
   - **Acc. code**
   - **Toll restriction**

     The toll restriction flag is only relevant for the route type PABX. It has no meaning for the route type CO; this means that it is not possible to disable toll restriction for CO trunks here.
   - **Emergency**

     NOTICE: Click on the blue arrow next to the **Route table** field opens the associated routing table.
5) Click on **Apply** followed by **OK**

16.2.3 LCR Routing Table

Least Cost Routing (LCR) is achieved by searching for a suitable route in the LCR routing tables (every trunk must be assigned a route). At the same time, the system checks if the class of service (toll restriction) matches for this route. The outdial rule is also dependent on the assigned path.

The routing table describes:

- the route assigned to the relevant path.
- the outdial rule,
- the LCR Class of Service (COS) required for seizure,
- the warning method for a more expensive route (warning tone).
- the dedicated gateway and
- the GW node ID.

The table is searched from top to bottom in hierarchical order. The system checks to determine whether the route is free and the station has the requisite LCR class of service. If this is the case, dialing occurs according to the dial rule entered in the route table if this is permitted by the toll restriction class of service and the CON group assignment between the subscriber and the line.

If the first route selection in the route table is busy, the LCR function can advance to the next (possibly more expensive) route configured in the route group table. The system can notify the user of this with an audible signal, an optical signal, or both.

Up to 254 route tables with 16 routes each can be created.

Dedicated Gateway

A dedicated gateway is a fixed partner node in an IP internetwork (Dedicated Gateway -> Forced). When a dedicated gateway with the corresponding GW node ID is entered for the IP networking route, routing to this gateway is enforced.

In a multi-gateway configuration, a dedicated gateway is determined via the subscriber configuration.

16.2.3.1 How to Edit Routing Tables

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **LCR**.

3) Click on **Route table**.

4) All routing tables are displayed for you:

- **1-Table**
- **2-Table**
- **nn-Table**

INFO: Routing tables 1 to 15 are intended for default entries or for configuration using wizards. During a migration, the

existing entries are automatically entered into these routing tables.

However, this mechanism does not prevent any duplicates in the entries. Manual post-processing of the routing tables is therefore recommended.

5) Click on the desired routing table. The selected table with the **Change Routing table** tab is displayed.
6) The individual routing tables are listed under **Change Routing table** and you can edit the following fields:
   - **Route**
   - **Dial Rule**

     NOTICE: By clicking on the blue arrow next to the desired rule, you can view and edit the dial rule properties.

   - **min. COS (LCR Class of Service)**
   - **Warning**
   - **Dedicated Gateway**
   - **GW Node ID**
7) Click on **Apply** followed by **OK**.

16.2.4 LCR Class of Service

Every subscriber is assigned a separate LCR class of service (COS). A subscriber can only seize a route if his or her COS is greater than or equal to the LCR COS in the route table, i.e., a subscriber with a COS 7 cannot seize a route with COS 8. By default, all subscribers are entered with the maximum LCR Class of Service (15).

Dependencies

Topic	Dependency
Toll restriction	The Toll Restriction class of service has precedence over the LCR class of service. The Toll Restriction class of service can be enabled and disabled for tie trunks.
CON Group Assignment	Dialing occurs only if allowed by the CON matrix.

16.2.4.1 How to Assign and Change an LCR Class of Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Classes Of Service**.
4) Assign an LCR class of service under **Edit LCR Class of Service** in the **Class of Service** field or edit an existing class of service.

   This only applies to the class of service of a subscriber for LCR. The field has no effect on the toll restriction.
5) Click on **Apply** followed by **OK**.

16.2.5 LCR Outdial Rules

LCR outdial rules can be used to convert the phone numbers entered into random new digit strings for additional processing. Access to different carriers is enabled via digit translation. The dial rule used is defined by the path or the route in the route table.

System-Specific Information

The communication system can administer up to 254 outdial rules in the LCR dialing rules table. The name of a dial rule can contain up to 16 characters.

The dialing rules address the dial plan fields selectively for the following operations:

- Repeating digits
- Suppressing digits
- Exchanging digits
- Inserting digits
- Switching the signaling method
- Detecting a dial tone
- Inserting pauses

Dial Rule

You can define up to 254 outdial rules here with a maximum length of 40 characters each.

The LCR dialing rules table is also referred to as the routing table.

Definition of Outdial Rules (Dial Rule Format)

- A:

  Repeat remaining fields (transmit). The letter "A" causes all subsequent digit fields to be transmitted. The point of reference is the last field delimiter in the field of dialed digits in the dial plan.

  If "A" is entered without an explicit reference, it designates all digits after the acces code, i.e., "A" is then equivalent to "E2A".
- B:

  It is used for the multi-gateway network when a station number of type TON (Type Of Number) that was called from outside is "unknown" and must be routed to the multi-gateway node. To ensure that this station number is unique, it is extended to national or international in accordance with the TON

in the LCR. This is required when the DID numbers are not unique and need to be configured in the national or international format.

- D (n):

  Dial digit sequence (1 to 25 digits). "D" may occur multiple times and at any position in the string.
- E (n):

  Transmit field contents (1 to 10). "E" may occur multiple times and at any position in the string. "E" can also appear in any order with relation to (n). A specific field can be addressed multiple times, including in sequence. With the exception of "E1" (access code), this letter can be surrounded by any parameters.

  With digit-by-digit dialing (opposite of en-bloc dialing), the last element in the outdial rule cannot be E(n); it may be E(n)A.
- M (n):

  Authorization code (1 to 16). This letter must not be in the final position.
- P (n):

  P (n) can occur more than once in the string and can be placed in any position. P (n) can be surrounded by any other parameters.(1 to 60 times the system-wide pause unit).
- S:

  Switch, changes signaling methods from DP to DTMF (with CONNECT, PROGRESS or CALL PROC with PI). The letter "S" may occur in the string only once and must not be in the final position. The "C" parameter cannot be used after "S".
- C:

  Carrier "C" can be inserted in the string only once. The subsequent characters are transmitted without a dial pause and are used for single stage, two-stage, DICS (not for U.S.), BRI, and PRI carrier access.
- U:

  Use subaddress signaling method. The letter "U" may occur in the string only once and must not be in the final position. The "S", "P", "M", and "C" parameters cannot be used after "U".
- N (n) (only for the U.S.):

  Network SFG (1 to 5) or Band Number (1).
- L (for U.S. only!):

  "L" must only occur at the end of a string of characters. "L" causes the call to be handled as an emergency call.

Example:

The system should automatically add a provider suffix.

Dial rule D010xxA means: the system first dials the Provider prefix (010xx), and then all the digits after the access code dialed by the subscriber (A).

16.2.5.1 How to Edit the Outdial Rules

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial rule**. All outdial rules are displayed for you.
4) Click on the desired dial rule in the menu tree.
5) You can edit the following fields:
   - **Rule Name**
   - **Dial rule format**
   - **Network provider's method of access** (**Unknown**, **Main network supplier**, **MCL Single Stage**, **MCL Two Stage**, **Corporate Network**, **Dial In Control Server**, **Primary Rate Interface**)
   - **Type** (**Unknown**, **Country code**, **Area code**, **PABX number**)
6) Click on **Apply** followed by **OK**.

16.2.6 Network carriers

You can assign network carriers to each route. The selection of the network carrier is defined by the LCR outdial rules.

Unknown

No explicit specification about a network carrier.

Main network supplier

When seizing a trunk using the main network supplier, simplified dialing into the public network is performed by en-bloc dialing or by dialing individual digits.

MCL Single Stage

With MCL Single Stage, a prefix is used to dial the desired network carrier, and the station number is then dialed. Dialing occurs in the D channel for ISDN or as normal dialing for MSI.

MCL Two-Stage

With MCL Two Stage, a prefix is used to dial the desired network carrier. After a synchronization phase, a configurable authorization code is initially sent followed by the destination call number as DTMF digits.

With synchronization during timeout, you must program a pause of 2 to 12 seconds.

Corporate Network

A corporate network is directly connected to the communication system. The LCR function determines the appropriate trunk group based on the station number dialed and then routes the call either via the trunk group in the public exchange or via the trunk group in the corporate network.

Dial-In Control Server

With this type of LCR, the desired network carrier is dialed with a prefix via a dial-in control server, and the call number and configurable authorization code are transmitted in the subaddress. Dialing occurs in the D channel.

Primary Rate Interface (PRI) (U.S. only)

In the case of the Primary Rate Interface, the selection of the network carrier or of a calling service is encoded in SETUP message using following information elements: Network Specific Facility, Operator System Access and Transit Network Selection.

Dependencies

Topic	Dependency
Receiving/forwarding call information	Temporary or permanent station number suppression cannot be activated.
ISDN/SUB addressing	The ISDN feature SUB must be applied for or released in the public network.

16.2.7 Selective Seizure of Exchange Lines

Exchange lines (aka "outside lines" or "CO trunks") can also be seized selectively by subscribers.

The prioritization for the seizure of exchange lines is handled via Least Cost Routing by default. In most cases, the least-cost provider is selected first, followed by the second-lowest cost provider, and so on.

If a subscriber wants to conduct a call over a provider that is not first in the LCR (because this provider is cheaper for long-distance calls, for example), he or she can select this provider via a specific trunk code or trunk key.

Subscribers can likewise also use selective dialing via seizure codes to reach a number that can only be dialed using ISDN (in cases where Vodafone is otherwise preset as the provider, for example).

By default, the seizure code 88 is configured for the seizure of an outside line via ISDN. All codes can be configured later by the administrator or edited as required.

16.2.7.1 How to Configure the Code for the Selective Seizure of ISDN Trunks

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan**. The individual dial plans are listed.
4) Enter the desired name for the dial plan under **Name**.

5) Under **Dialed digits**, enter the seizure code and identifiers precisely (e.g., **88CZ**).

NOTICE: 88 is the default seizure code assigned by the system for the selective outside line seizure of an ISDN trunk.

For information about the abbreviations C and Z, see LCR Dial Plan .

---

6) Under **Routing table**, enter a **1**.
7) Click on **Apply**, followed by **OK**.

16.2.7.2 How to Display the Seizure Code for the 'Outside Line Seizure'

The **CO Trunk ISDN / Analog / ITSP** wizard can be used to selectively display the codes for ISDN trunk seizure.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Your communication system is connected to an analog trunk.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **CO Trunk ISDN / Analog / ITSP** wizard.
4) Continue clicking on **OK & Next** as often as needed until you reach the **Seizure Code for the 'Outside Line Seizure'** window.
5) In the default view, you will see the code for the ISDN trunk seizure. For configured ITSPs, the corresponding codes are shown.
6) Click on **OK & Next** followed by **Finish**.

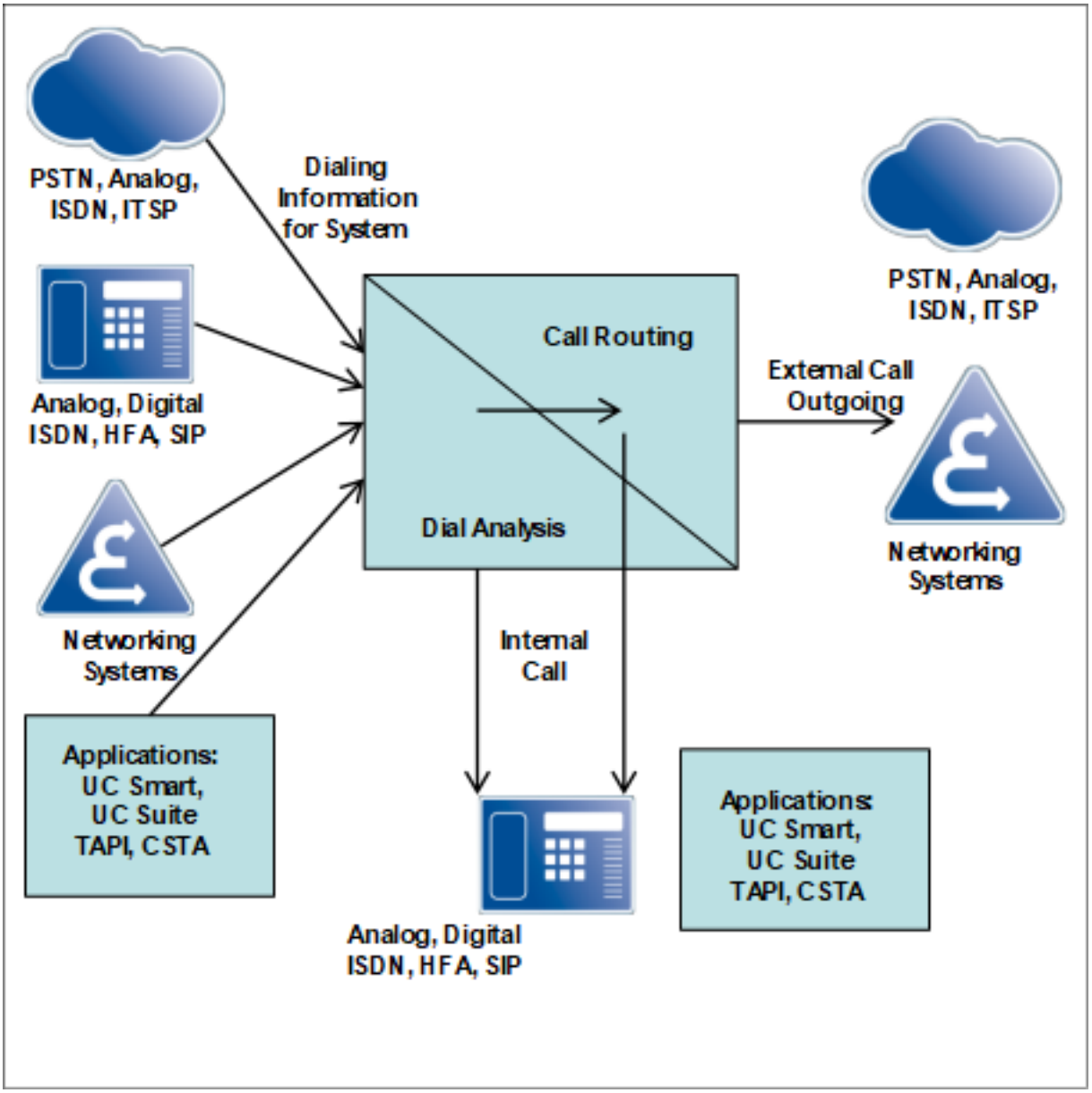
16.3 Digit Analysis and Call Routing

This section illustrates the relationship between digit analysis and call routing. It explains how the communication system analyzes call numbers dialed by subscribers, trunks and applications of various types to reach a specific destination and how the calls are routed upon completion of the digit analysis. The relevant system functions for this have already been described for the most part in the previous sections. This section describes dialing with public phone numbers within a node/network in detail.

The Digit Analysis

- of the communication system records and evaluates all dialed numbers on the basis of the configuration data
- verifies classes of services (e.g., based on classes of service for stations, station flags, day/night, allowed and denied station numbers, LCR classes of service, schedules, connection matrices, etc.).

- determines whether a number can be dialed internally or whether a line is to be seized. This applies to the dialing of internal and public call numbers as well as for network-internal call numbers.
- normalizes call numbers so that they can be dialed by the communication system. (e.g., canonical format: "+49nnn" becomes "00049nnn", where the first ’0’ is the main access code of the PBX)
- truncates call numbers where necessary (the leading digits of destination numbers may have to be truncated for calls with inbound trunk seizure in order to determine the DID destinations in the short format)



16.3.1 Overview of Call Routing / LCR

An incoming call is subjected to various tests in the communication system and then forwarded accordingly.

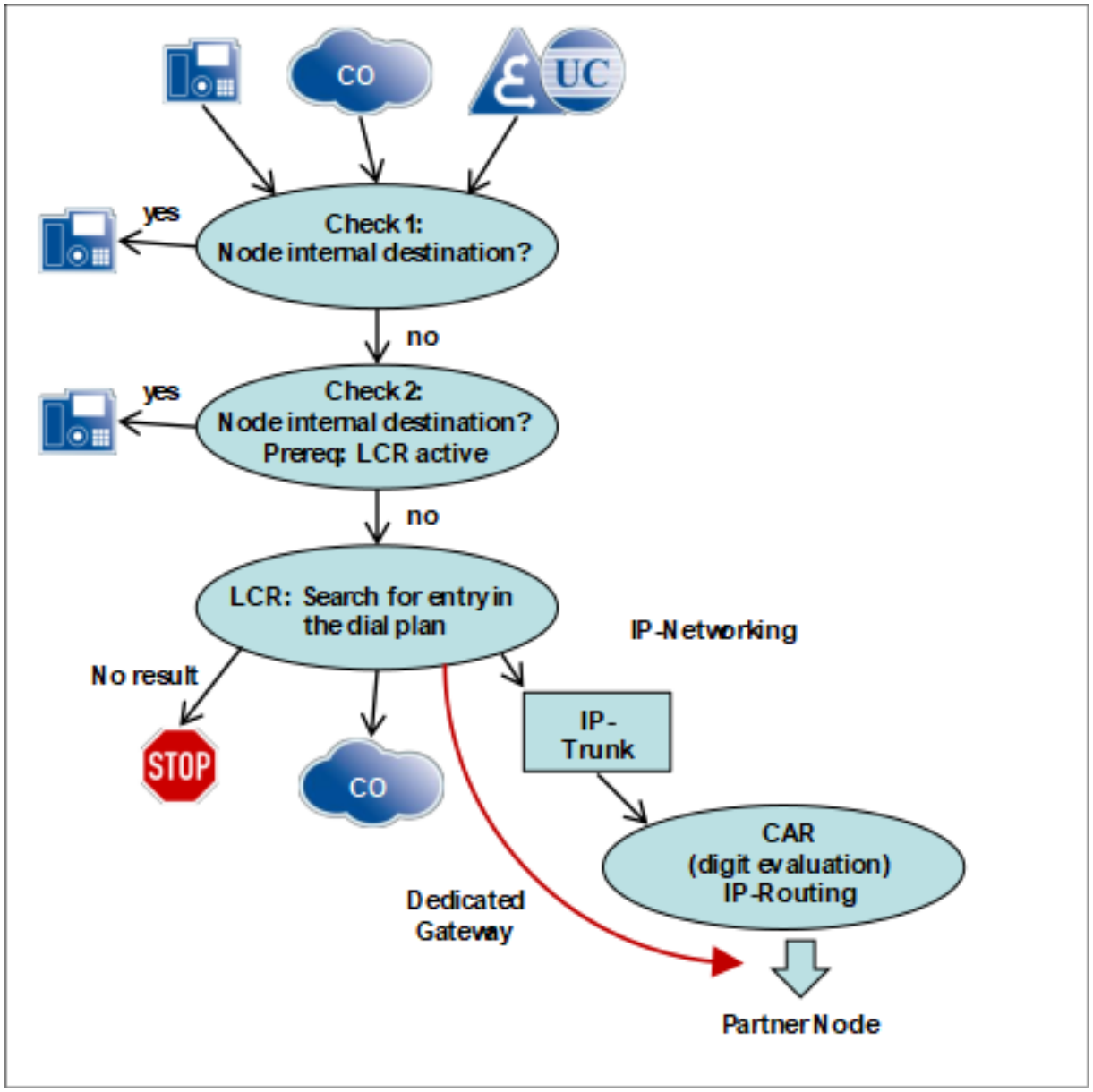
Test 1 (internal call destination?)

- Destinations with canonical call numbers are first converted into dialable numbers (at the station interface) or set to TON=International (ITSP interface).
- For trunk destination numbers, the call number portion of the PABX number of the corresponding route is stripped off if required.
- Internal calls are analyzed on the basis of the internal dial plan; for external calls, the dial plan for DID numbers is used.

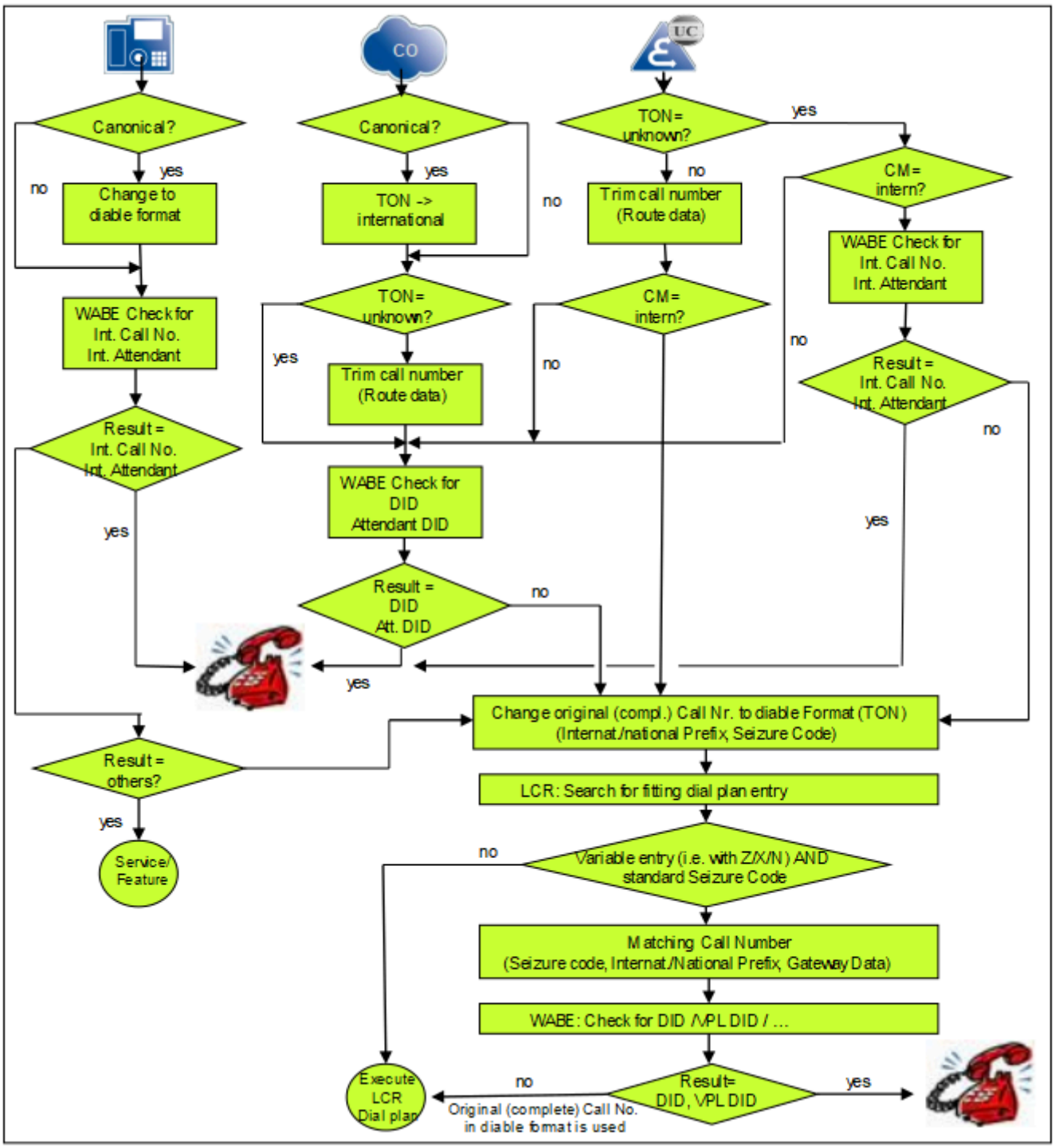
Test 2 (internal call destination?)

- Subscribers, applications, clients or other communication systems use the public format (for example, 00049nnn) for dialing destination numbers
- Precondition: the default CO access code (e.g., "0") has been set up.
- The destination number is stripped to remove the location number (gateway location) portions and evaluated based on the dial plan of the DID numbers, regardless of whether an internal or external call is involved.
- If no internal call destination is found, the dialable, unstripped (!) call number is processed in the LCR, and the call is routed further over a line accordingly.

Within an IP network, the LCR routing table parameter "Dedicated Gateway" enables the direct addressing of a node for a dialed number by bypassing the CAR digit analysis.


CO
UC
yes
Check 1:
Node internal destination?
no
yes
Check 2:
Node internal destination?
Prereq: LCR active
no
LCR: Search for entry in
the dial plan
IP-Networking
No result
STOP
CO
IP-
Trunk
CAR
(digit evaluation)
IP-Routing
Dedicated
Gateway
Partner Node

16.3.2 Digit Analysis Flowchart



Explanations for the flowchart:

German	English	Explanation
WABE		Digit analysis

German	English	Explanation
CM	CM	Classmark identifies the caller as an external caller or (network-) internal caller
TON	TON	Type Of Number (Call number type): Unknown, Subscriber, National or International; used for both destination numbers as well as originating numbers.
DuWa	DID	DID number
TNR RNR	Int. Call No.	Internal number
Int. Attendant	VPL INT	Attendant number for internal calls
VPL DID	VPL DID	Attendant number for external calls
SERVICE	SERVICE	Service code
LCR	LCR	Least Cost Routing

For digit analysis, UC clients are treated as subscribers controlled via CSTA.

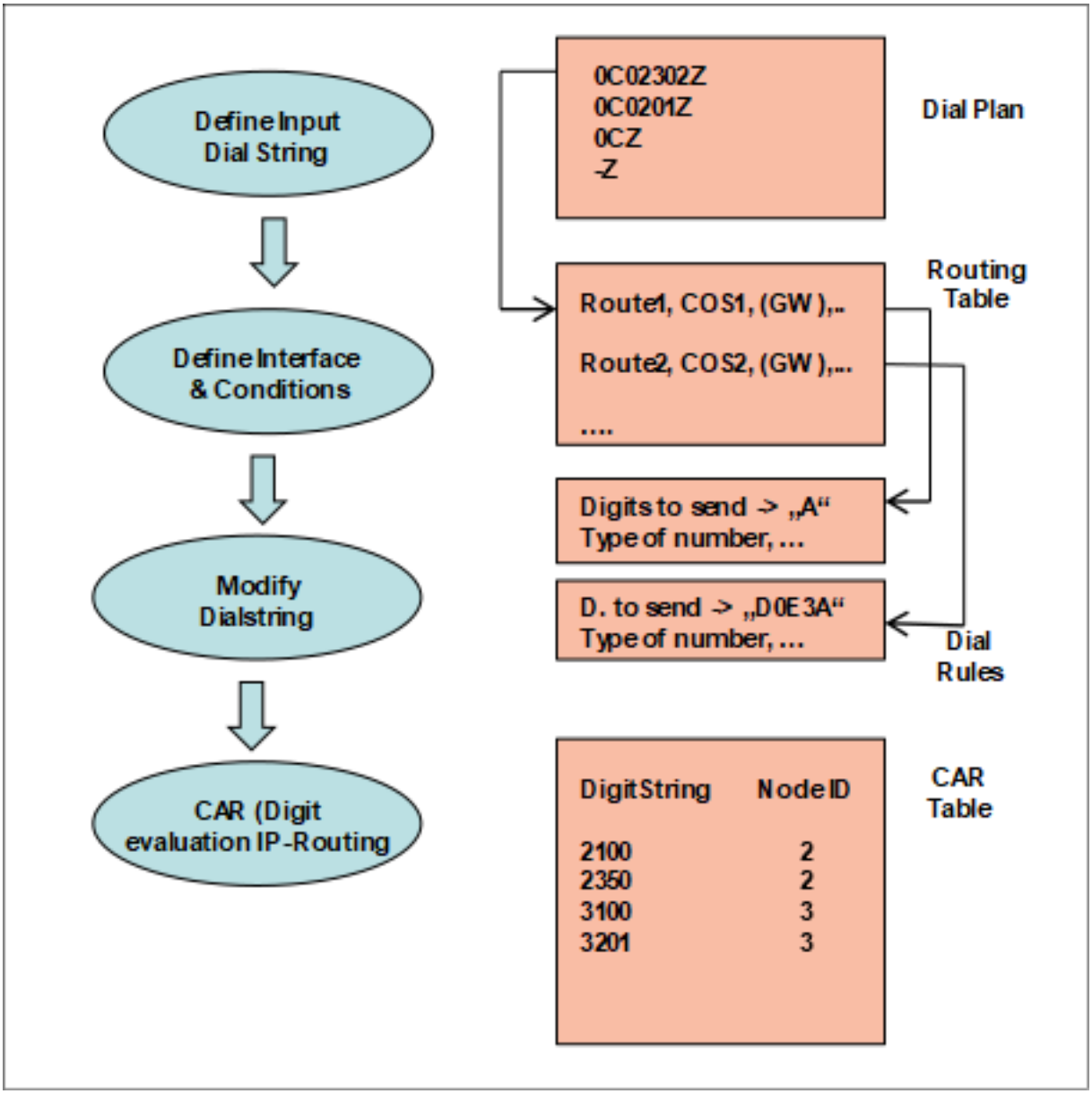
For digit analysis, the UC Suite behaves as a SIP-Q trunk.

16.3.3 Call Routing and LCR in the Internetwork

Call routing and LCR play an important role in networking. Calls are routed by using a dial plan and dial rules. The dedicated gateway plays a special role here.

LCR Basics

LCR Entries During the Initial Setup



If no line seizure is successful, the entries in the routing table are processed sequentially in a loop.

NOTICE: -z rule must be removed from stand-alone system configuration.

When the communication system is started up for the first time, a number of country-specific default values are entered in the LCR dial plan. Up to and including dial plan 35, system-side entries for emergency calls, directory assistance, special numbers, default trunk seizure for PSTN and ITSPs, for UC Suite and networking, and for international dialing formats are preset to ISDN trunks.

This range can be affected by configuration changes elsewhere (for example, by changes to the **Location number** flag. Consequently, whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected (which is important when dialing public numbers).

INFO: From LCR dial plan 36 onwards, all entries are freely available.

16.3.3.1 Dedicated Gateway

The dedicated gateway is only relevant for an IP network.

Why is a dedicated gateway required?

How can destinations be permanently set up through configuration?

Use cases for a dedicated gateway

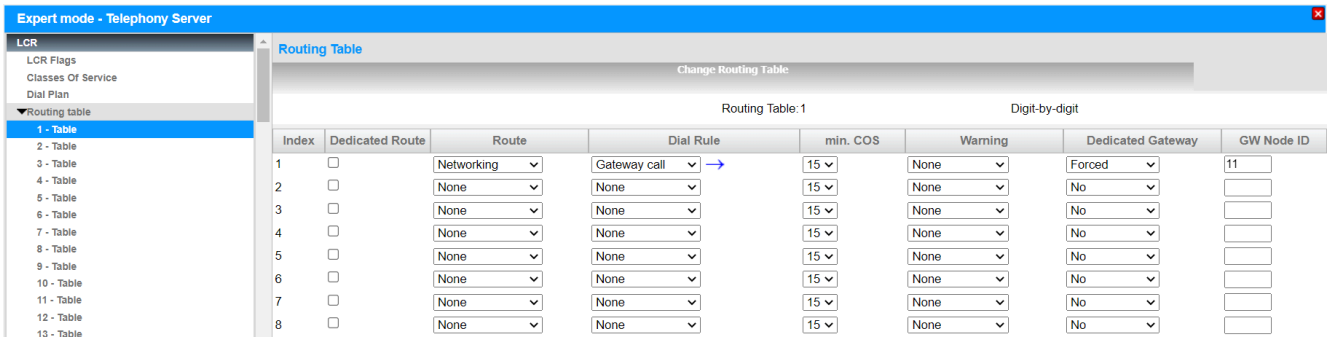
The Dedicated Gateway in the WBM

The following values can be set:

- The CAR table of each communication system includes network-wide numbers of the other nodes and is automatically refreshed (overwritten) cyclically during updates. Consequently, CAR tables are not suitable for the permanent use of manually added entries.
- Only numbers that apply network-wide are entered, i.e., no node-specific routing is possible (e.g., "0" to the respective gateway node)
- By using direct addressing in the LCR
- The dedicated gateway directly addresses the destination node using the node ID (IP address)
- When using the dedicated gateway, CAR tables are bypassed (see previous figure).

Direct addressing

- of TDM gateways to seize outside lines ("0CZ")
- of TDM gateways to implement breakouts via separate codes
- of internal network nodes that are to be reached via public numbers
- of TDM gateways to which the subscribers of a multi-gateway network (to an OpenScape Business S) are assigned (e.g., subscriber 1 belongs by definition to gateway 1, and subscriber 2 belongs to gateway 2).
- of gateways and calls whose origin CANNOT be associated with a specific gateway in a mult-gateway configuration (e.g., the fax group of a UC Contact Center)



No	The station number analysis occurs on the basis of the CAR tables (no **GW node ID** required)
Forced	Routed directly to the appropriate gateway (GW node ID = n)
Multi Location	Only to be used with multi-gateway configurations: Based on the multi-gateway configuration of the OpenScape Business S subscribers, the communication system knows the assignment to their respective gateways and can selectively route outbound calls to the appropriate gateway. In the **Multi Location** configuration, the GW node ID is used only if no gateway can be identified through the assignment of the subscriber (default).

16.3.4 Scenarios: Digit Analysis and Call Routing

In order to illustrate the above processes in the communication system, the dependencies and required configuration parameters are described here on the basis of specific scenarios. The presented scenarios may build on one another, depending on the use cases involved.

Single System

Networked system as a subsystem (no CO trunk)

Internetwork with multi-gateway

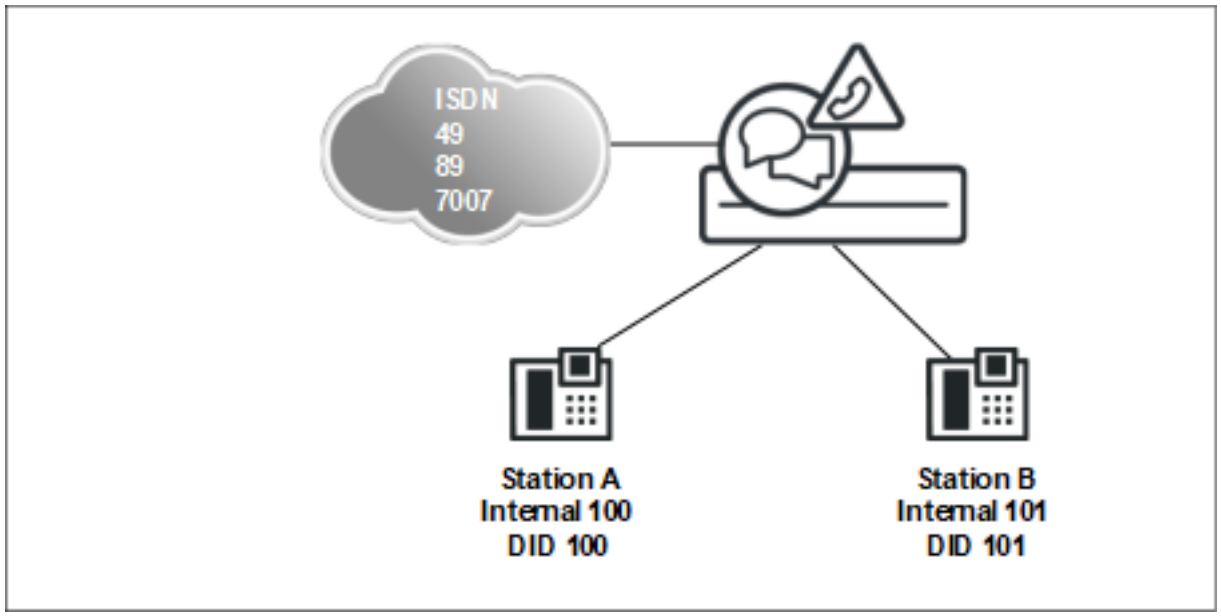
1) Subscriber A calls subscriber B via an internal phone number
2) Subscriber A calls subscriber B via a public phone number
3) Subscriber A calls an external station via the CO
4) ISDN trunk calls subscriber A
5) Special configurations and their corresponding effects

2 CO routes

1) Subscriber A Calls Subscriber C via an Internal Phone Number
2) Subscriber A calls subscriber C via a public number in the internetwork
3) ISDN trunk calls subscriber C

1) ISDN trunk gateway 1 calls subscriber D
2) Subscriber D calls external station via the CO

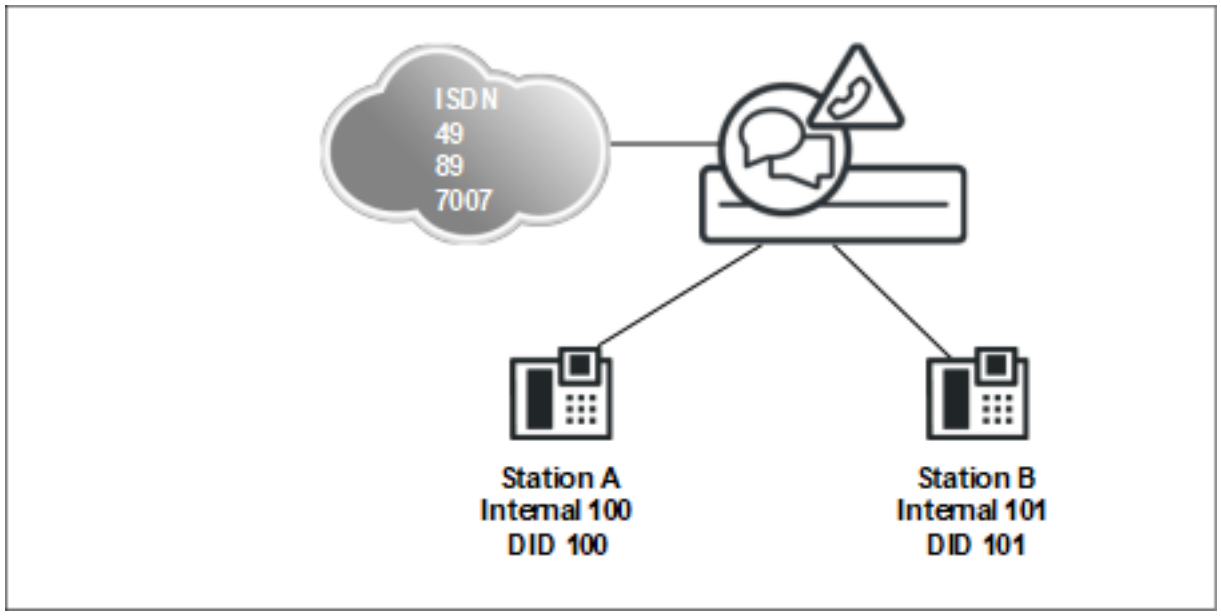
16.3.4.1 Subscriber A Calls Subscriber B via an Internal Phone Number



16.3.4.2 Subscriber A calls subscriber B via a public phone number

Configuration

Dependencies of the "Location Number" (Gateway Location)



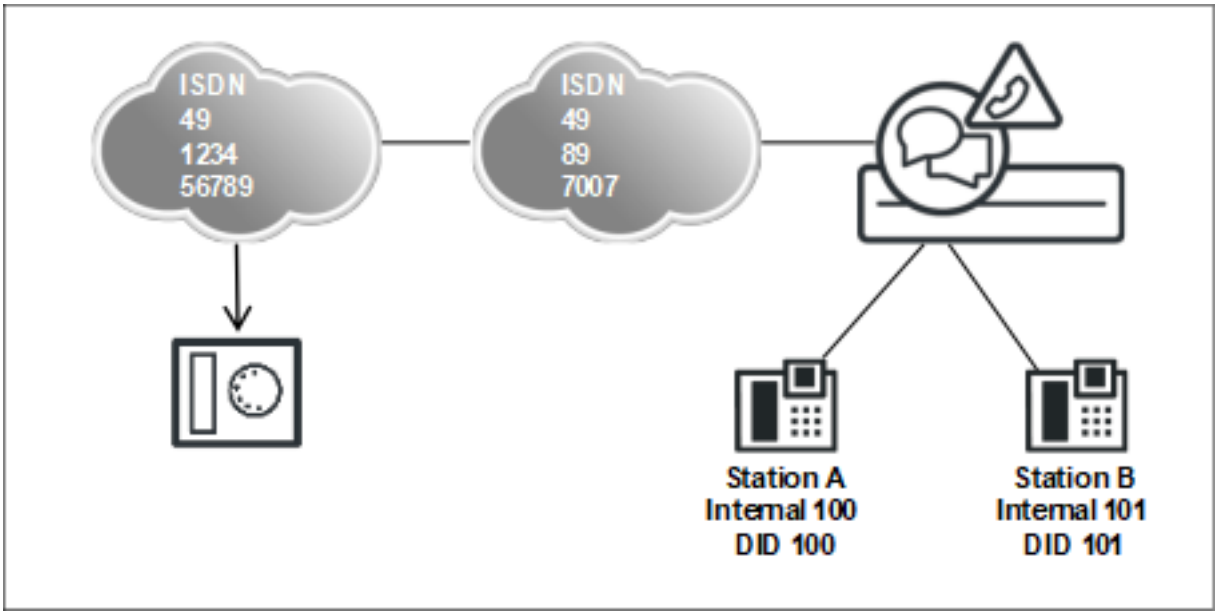
	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

The location number (gateway location) is analyzed on dialing based on the public phone number. If the relevant portions of the dialed number matches this number, the DID table is analyzed and, if a match is found, the appropriate internal destination is dialed (without seizing a trunk!). By setting the Location Number flag, the location data is taken over automatically from the appropriate routing data (PABX number, incoming) and does not need to be changed in standard scenarios.

Consequently, only valid numbers assigned to this system should be entered in the DID tables; otherwise, masking effects could occur with numbers in the public network. For example, in some cases, an internal number identified by an invalid DID could be called even though a call via a trunk to an external destination was intended.

Changes to the "Location Number" flag may affect the preset default LCR entries. Whenever the location number is changed, it must be ensured that the default trunk seizure still works as expected. This is important when dialing public numbers.

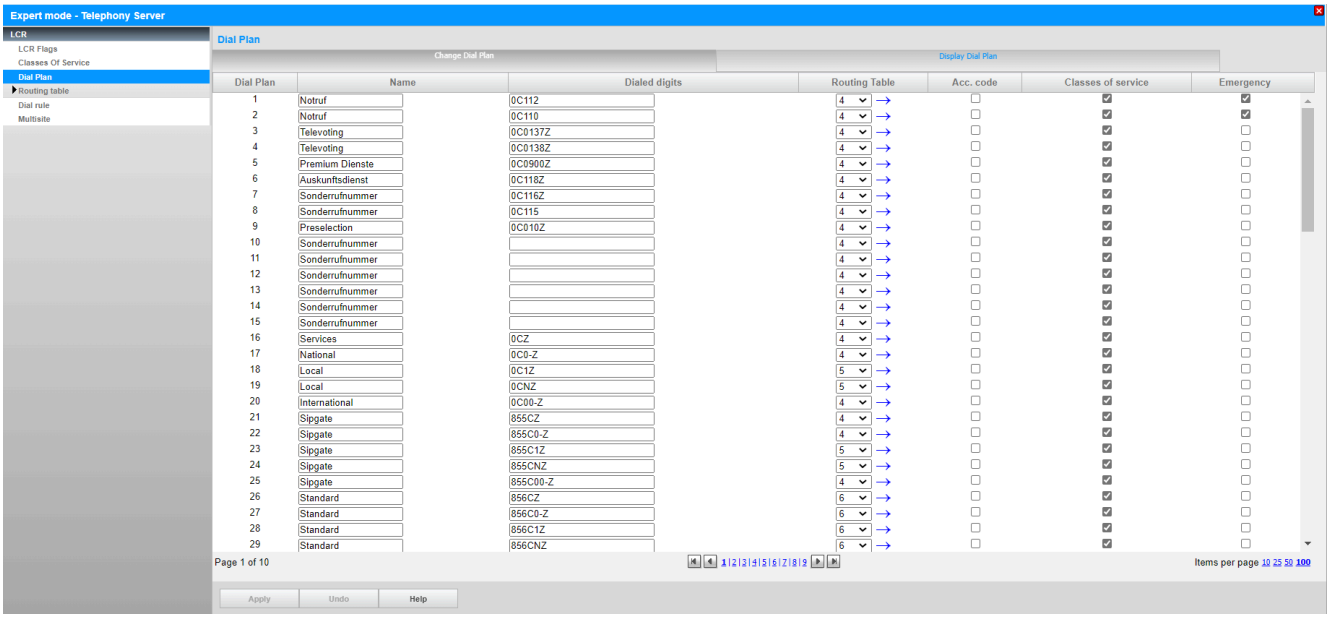
16.3.4.3 Subscriber A calls an external station via the CO



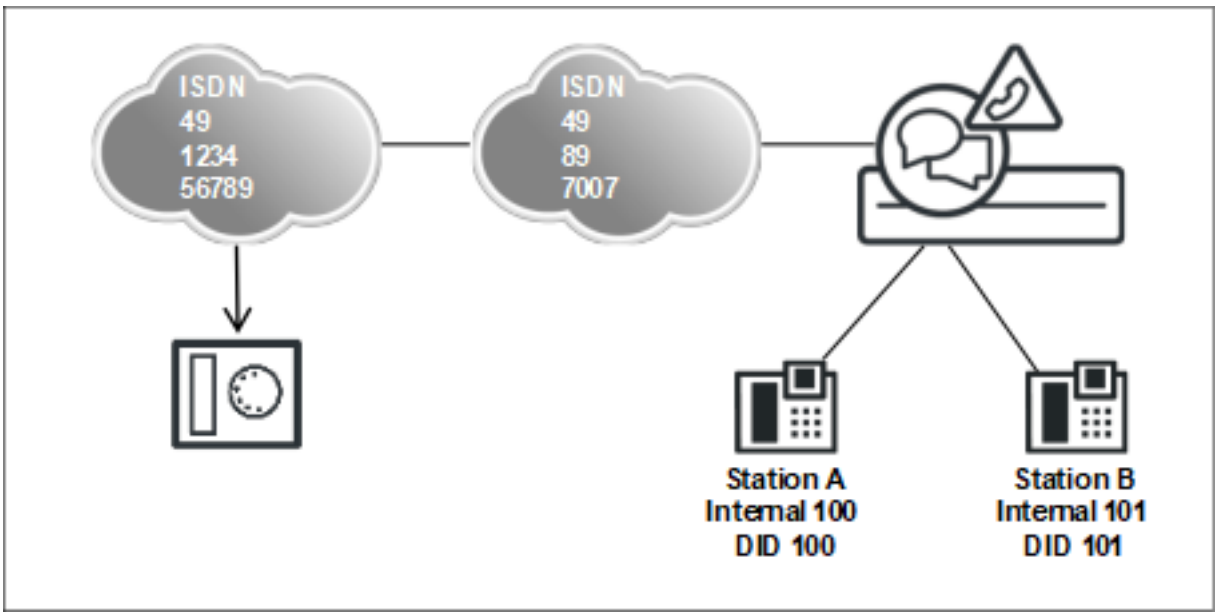
The call is routed via LCR because the destination is not in the own communication system.

In addition to the data of the previous scenario "Subscriber A calls subscriber B via a public phone number", a suitable dial plan entry to seize the CO trunk (e.g., "0CZ") must be present in the LCR.

The LCR route table and the dial plan must be set up accordingly.

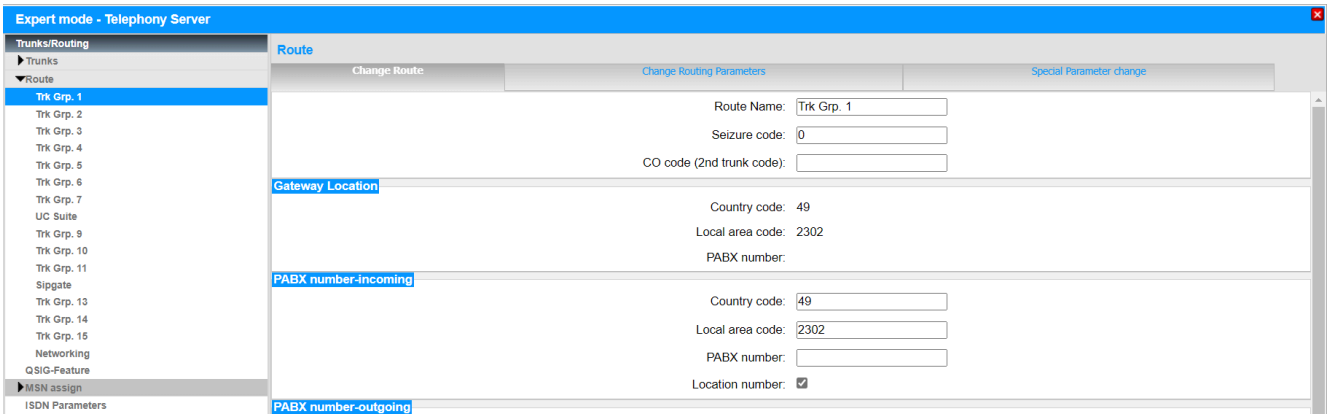


16.3.4.4 ISDN trunk calls subscriber A



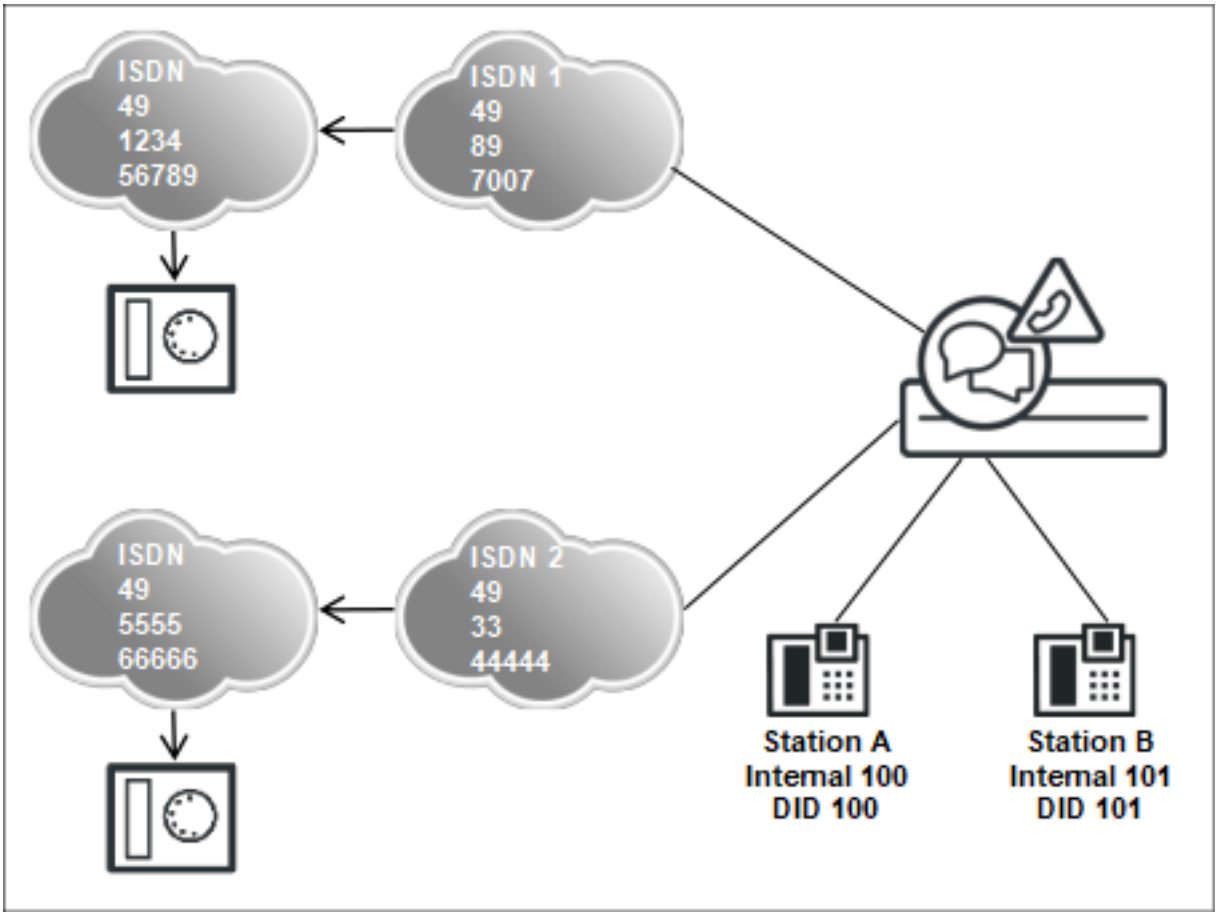
For an incoming call over an ISDN trunk, the route is stripped off from the destination number based on the configuration data of the PABX number, incoming. Using the remainder of the destination number (DID), a search for a destination is then performed in the DID dial plan.

The parameters of the gateway location and the **Location Number** flag play no role in this scenario.



16.3.4.5 Special Configurations

Special configurations and their corresponding effects: 2 CO routes



Example:

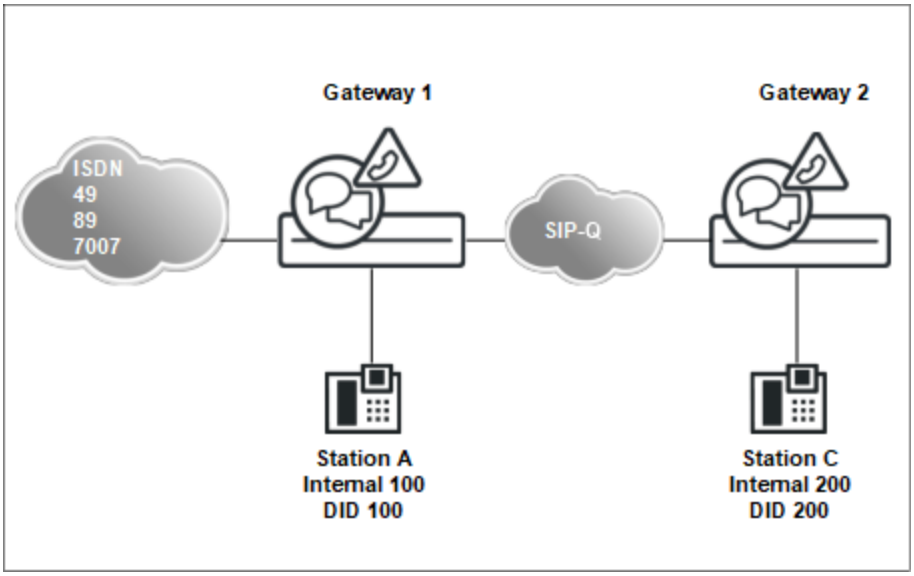
- A customer wants to use a standard ISDN 1 connection. This is set up as the location number.
- A second ISDN 2 connection is additively used for special applications.

Notes and limitations:

- Only ONE CO trunk (ISDN 1 = location of the system) is fully supported, i.e., no multi-tenant configuration (tenant services) with equal trunk access rights can be configured.
- The additive ISDN 2 CO trunk can be used for Basic Call (incoming/ outgoing).
- In complex switching scenarios, the correct representation of the call number may not be guaranteed under some circumstance.
- For connected applications, only the location number is supported, as is the case when dialing internal destinations with public numbers.
- The configuration with respect to the routing configuration and LCR can be derived from the previous examples.

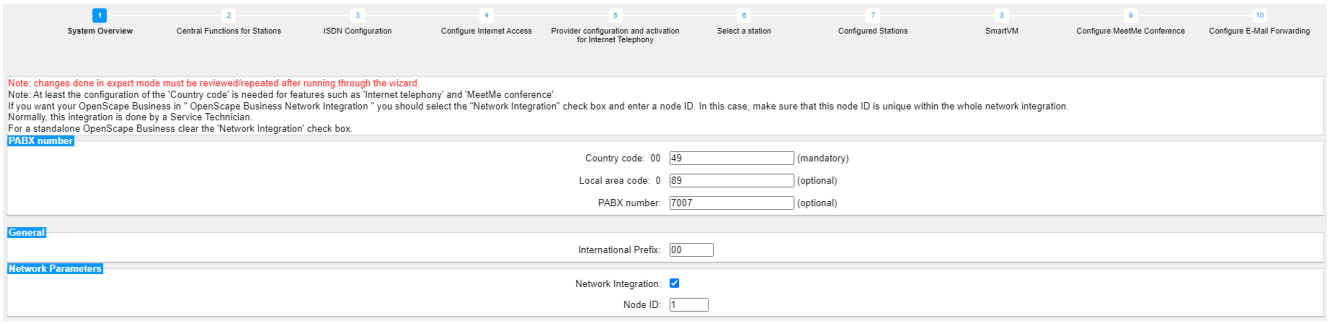
16.3.4.6 Subscriber A Calls Subscriber C via an Internal Phone Number

Networked communication system as a subsystem (no CO trunk)



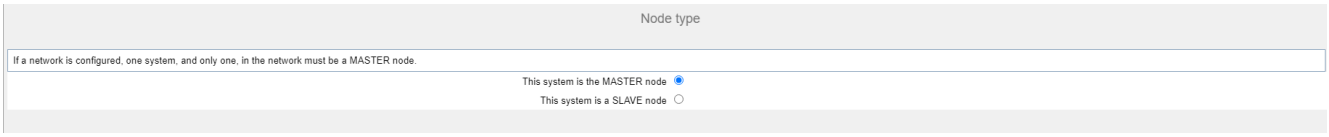
Prerequisites for standalone systems before networking:

- Both communication systems have unique IP addresses and are integrated in the IP network of the customer.
- Both communication systems can be administered in the customer network using WBM.
- A unique node ID for networking was assigned in the basic installation for each communication system (e.g., System 1 = Node ID 1 and System 2 = NID) 2).
- Defining the numbering in the basic installation of the systems 1 and 2: The numbering of the standalone systems must take the closed numbering in the future internetwork into account.
- This example assumes that closed numbering is being used (mandatory when using UC Suite!); the configuration occurs via the Network wizard. With open numbering (possible for UC Smart), the Network wizard is not used. It is also not used with a connection of OpenScape Voice and OpenScape 4000.



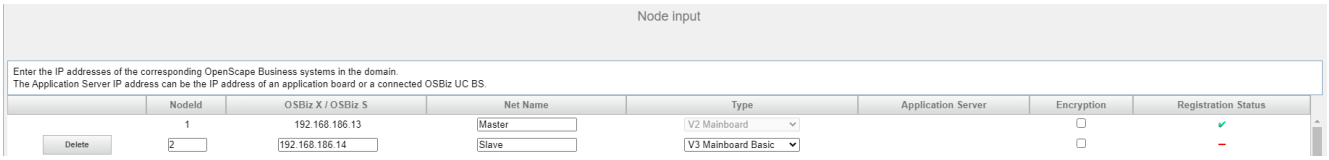
Start the Network wizard in system 1. This system (this node) is declared as the master). The master has several central functions in the network (e.g., administration, license management with centralized licensing, network-wide CSP).

If an OpenScape Business S is located in the internetwork, it should be preferentially declared as the master (for bandwidth and performance reasons).



The IP addresses are entered for each node so that the systems can find one another independently after the administration. The OpenScape Business systems are entered **Type**.

This dialog must also be completed for node 2 (slave).



Upon successful configuration, the two systems (nodes) synchronize their phone numbers and enter the call numbers of the other node into the CAR table.

With the creation of the CAR tables, network-wide telephony with internal numbers is possible. UC Suite is also launched network-wide. Further steps for the complete startup of the network are presented in the other scenarios.

CAR entries are controlled via **Expert Mode** > **Voice Gateway** > **Networking** > **Routing**.

An overview of the automatic synchronization in the internetwork can be seen in the WBM (sync status).

Additional network nodes can now be administered with direct access under the menu item **Networking** in the navigation bar.

16.3.4.7 Subscriber A calls subscriber C via a public number in the internetwork

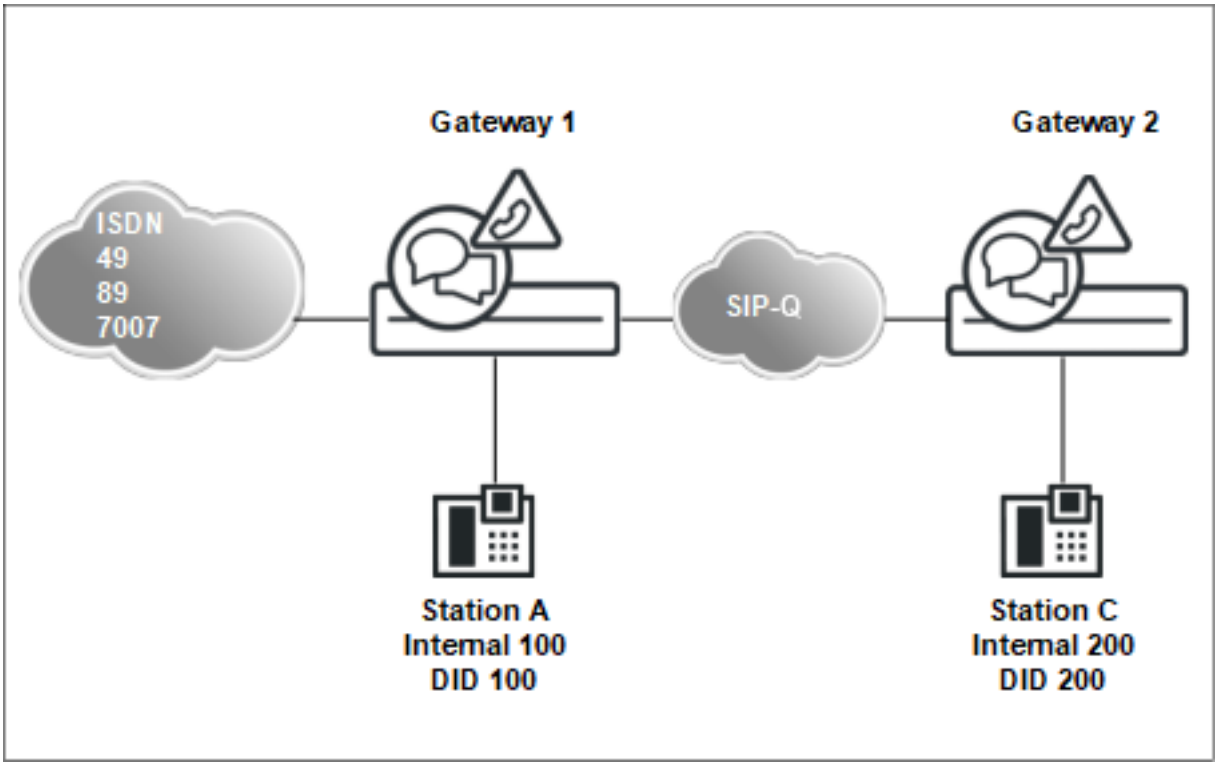
Networked communication system as a subsystem

Configuration of Node 1, Setup in the LCR via Dedicated Gateway

Configuration of Node 2, Setup of the "Networking" Route

Configuration of Node 2, Setup of the Location Number at the "Dummy CO Trunk"

Configuration of Node 2, Setup in the LCR via Dedicated Gateway



Special features of this scenario:

- System 1 detects that the destination phone number does not belong to the own system. A further search is thus performed in the LCR. The dedicated gateway in the LCR of system 1 must be used for the direct addressing of the node ID of system 2. The destination number is not an internal number of the network (it would otherwise be in the CAR table), but a public phone number, which can be dialed by the subscriber in three different lengths:

  Long = 00049897007nnn

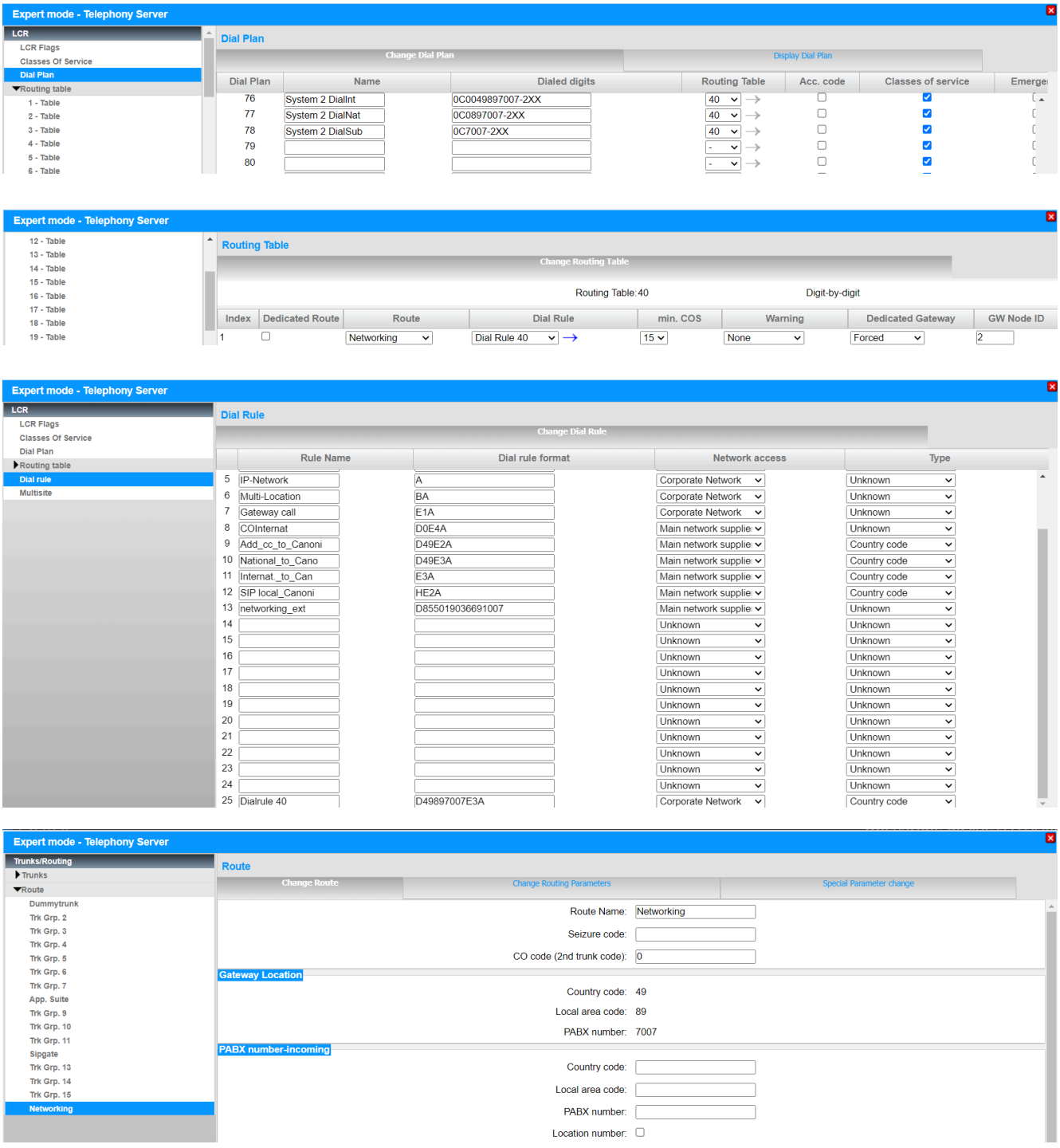
  Medium = 00897007nnn

  Short = 07007nnn

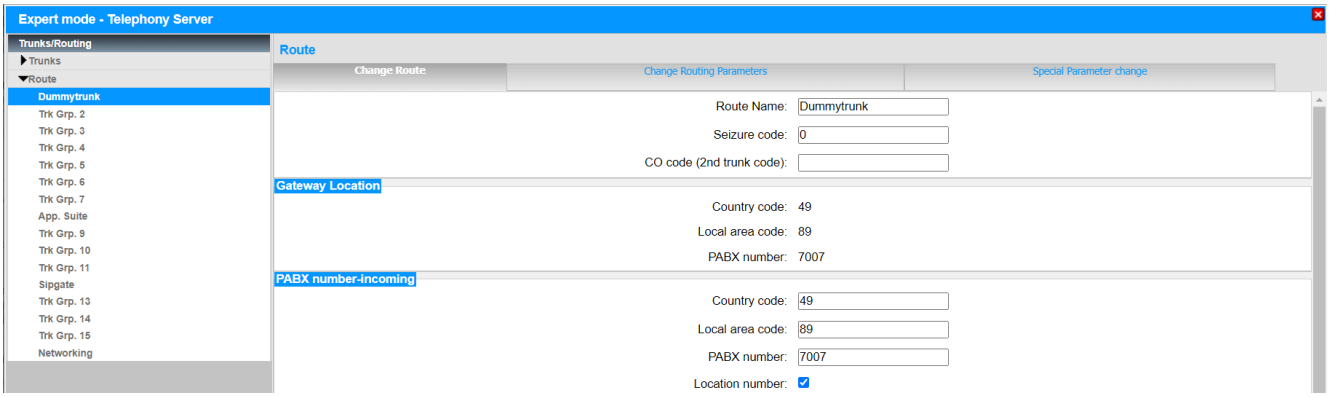
  This example assumes that all 2xx DID numbers are subscribers in system 2.

NOTICE: The dial plan entries must be configured precisely so that ALL numbers involved really belong to the subnode (internetwork). This may require a larger number of entries in a dial plan with peculiarities, e.g., when a shared trunk connection or an MSN configuration is involved.

- In node 2, a location number is entered with the location data of node 1 (gateway) using a "dummy CO trunk" so that the destination number from the public dialing can be stripped before searching for an internal destination in node 2.



The route type **PABX** must be entered on the **Change Routing Parameters** tab.



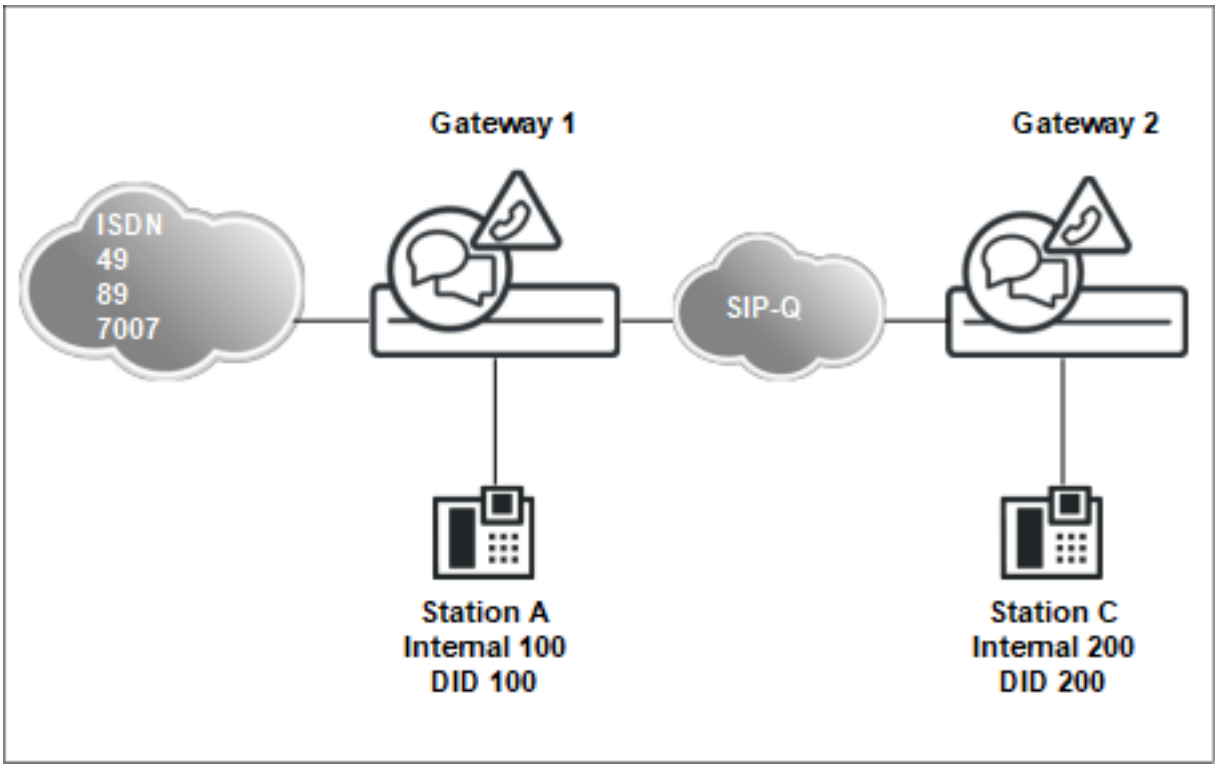
The route type **CO** must be entered on the **Change Routing Parameters** tab.

In node 2, all public numbers that do not belong to their own node are routed to node 1 (default dialing, e.g., 0CZ)

16.3.4.8 ISDN trunk calls subscriber C

Networked System as a Subsystem

Special Features of this Configuration



Example: Incoming call with destination number with TON = subscriber

- Node 1 must be set up as described in the previous scenario.

  The addressing of node 2 occurs with the public telephone number in both cases, regardless of whether the origin of the connection is located in node 1 (subscriber of system 1) or in the public network.

  INFO: The dial plan entries must be configured precisely so that ALL numbers involved really belong to the subnode (internetwork). This may require a larger number of entries in a dial plan with peculiarities, e.g., when a shared trunk connection or an MSN configuration is involved.

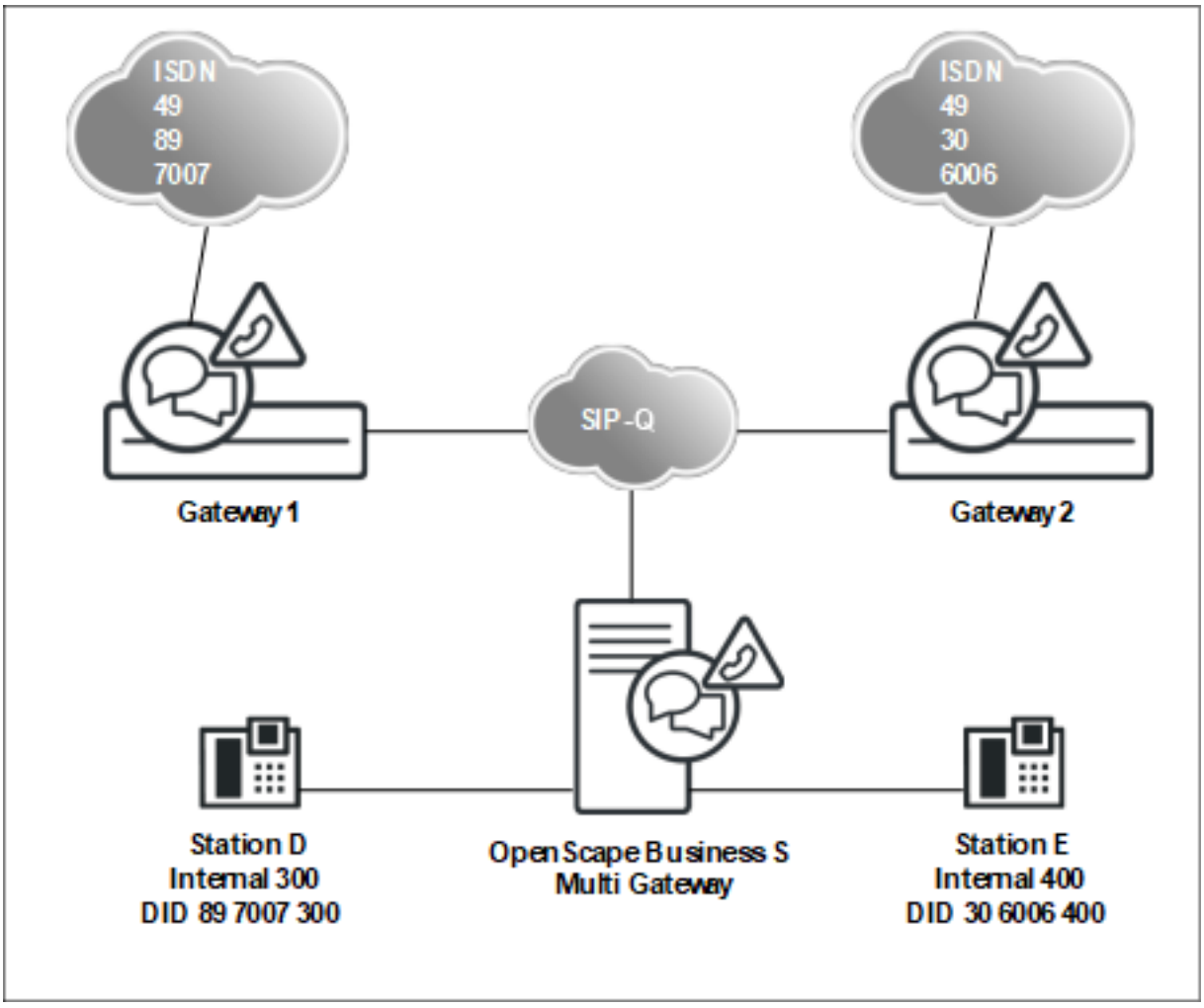
- Node 2 must likewise be set up as described in the previous scenario.

16.3.4.9 ISDN Trunk Gateway 1 Calls Subscriber D

Networked system in a multi-gateway configuration

Configuration

Configuring the Multi-Gateway, OpenScape Business S

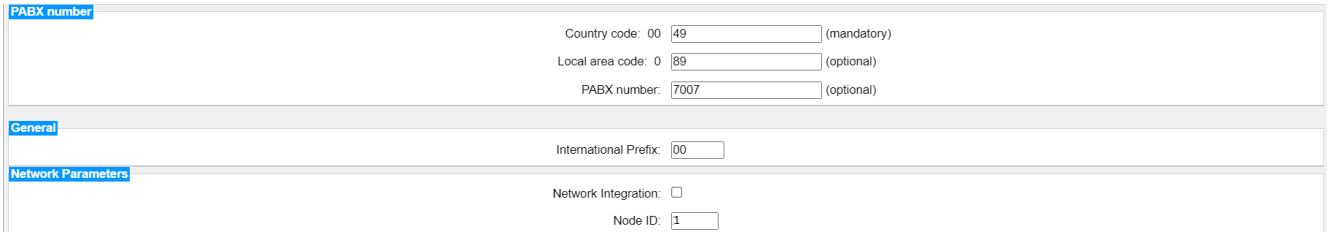


Example: Incoming call with destination number with TON = subscriber

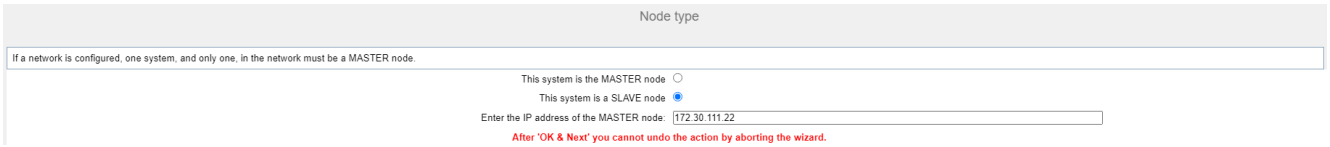
Special features in this scenario:

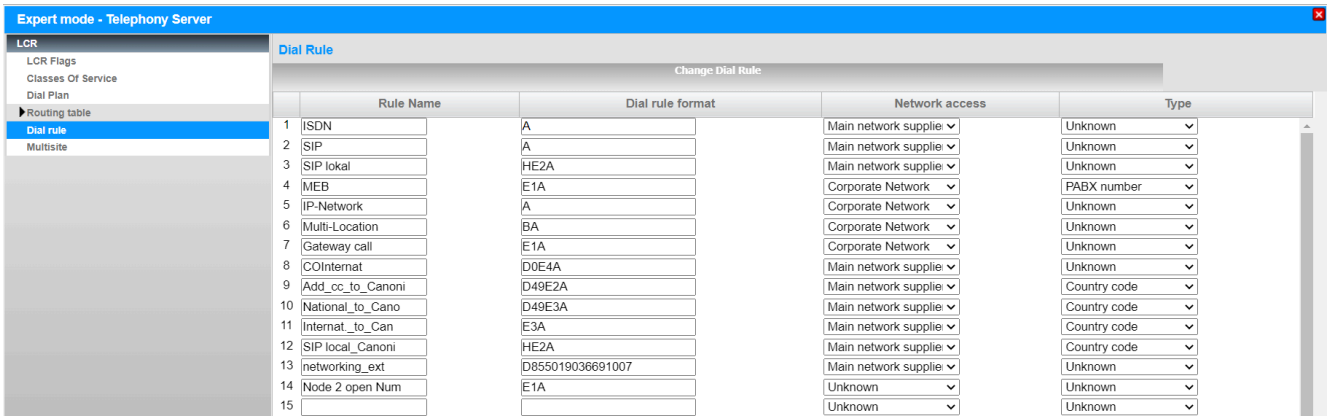
- Gateway 1 is basically set up as in the previous scenario (gateway 1), i.e., through the basic installation first and then by running the Network wizard. The essential difference here is that the gateways are set up as slaves, and the OpenScape Business S is set up set as the master (performance, bandwidth licensing).
- In this example, only the essential differences to the previous scenario are indicated.

Basic installation for gateway 1



Network wizard for gateway 1





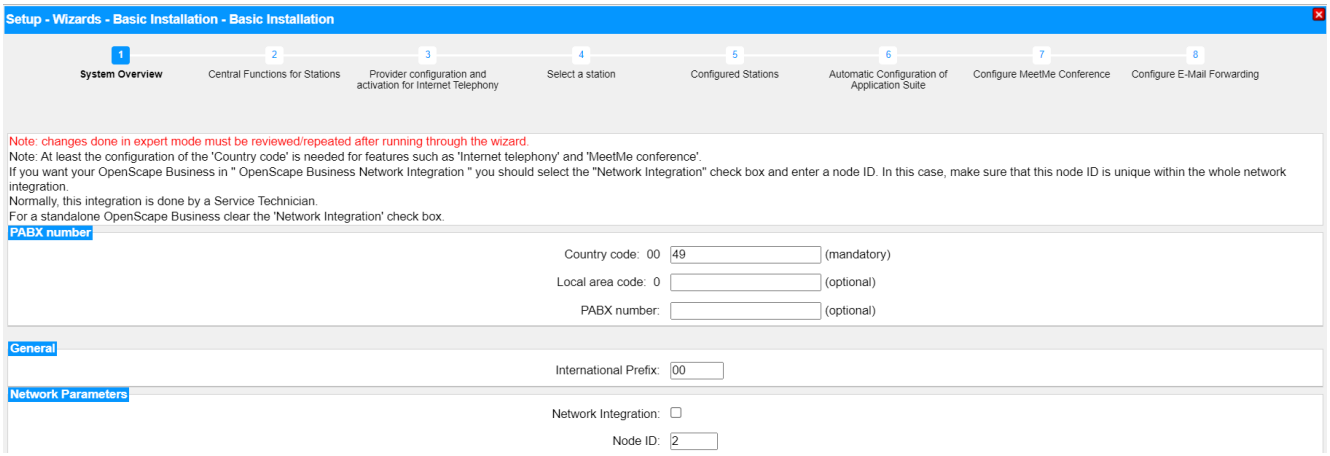
In the OpenScape Business S, the destination number is already entered as a DID in the "national" format.

"BA" (Broaden All) is significant only in the gateway.

"BA" is only needed when the original destination number TON unknown has been received, i.e., contains only the "short DID" = extension portion.

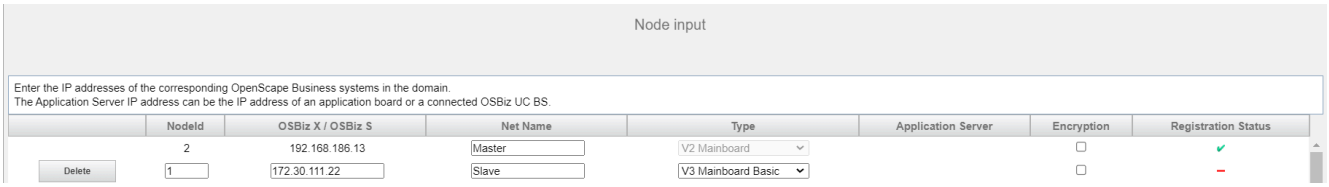
- After completing the basic installation first, the Network wizard is run.
- The following is set up for each subscriber of OpenScape Business S:
  - Internal number in short format (e.g., 300)
  - DID phone number in national format (e.g., 89 7007 300)
  - Associated gateway node ID

Basic installation of OpenScape Business S, multi-gateway



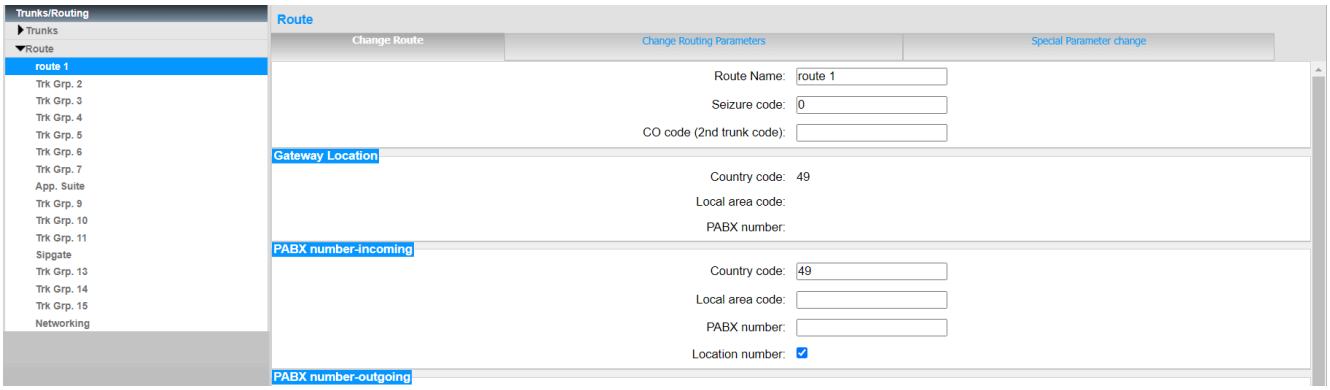
INFO: Only the country code needs to be entered in the system data; the rest of the complete call number is in DID entry of the subscriber.

Network wizard of OpenScape Business S, multi-gateway



Select multi-gateway in the network configuration.

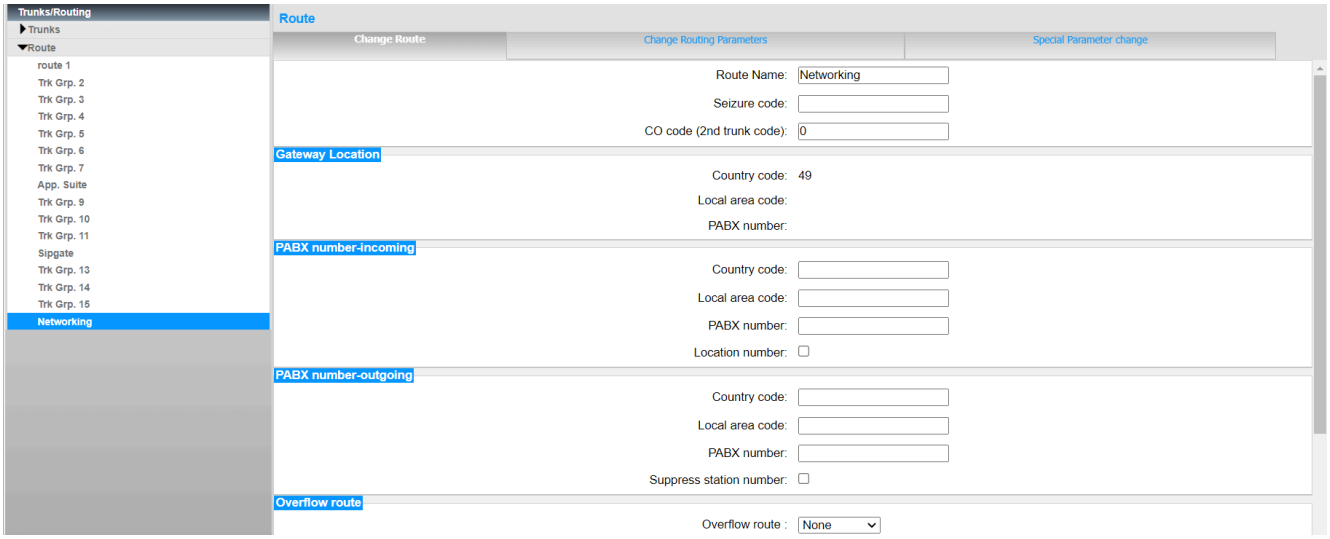
Routes of the OpenScape Business S, multi-gateway



The country code was already entered in the wizard.

Routing parameters: Route type CO (Central Office)

This route is assigned the route type "CO".



Routing parameters: call number type outgoing = National, Route type PABX

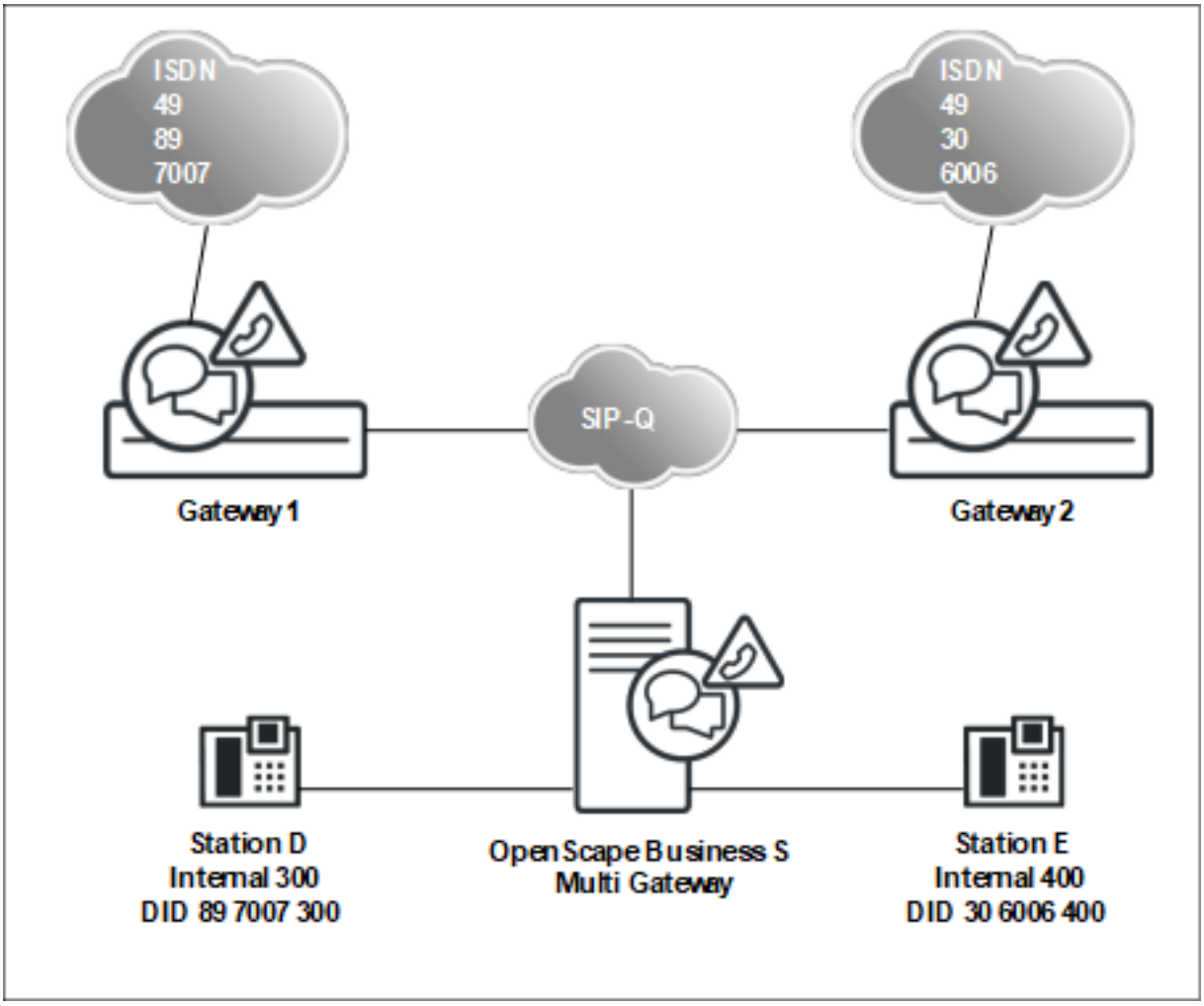
This route is assigned the route type "PABX", and the "No. and type, outgoing" must be set up with the **Local area code**.

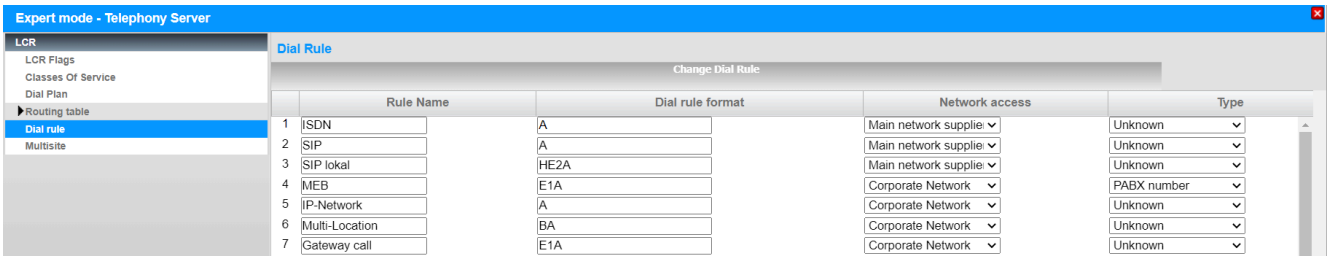
16.3.4.10 Subscriber D calls external station via the CO

Networked system in multi-gateway configuration

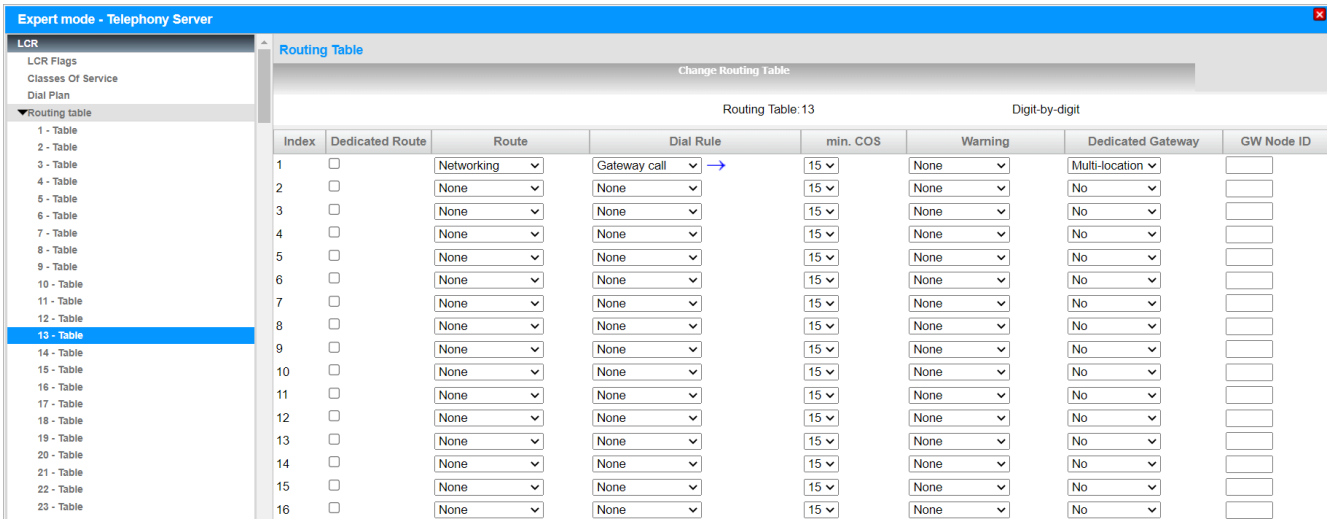
Configuration of the OpenScape Business S, multi-gateway

Routing of OpenScape Business S, multi-gateway, to the gateways





	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown



The setup of gateway 1 occurs as in the previous example. This also applies to gateway 2.

16.4 Emergency Calls

The communication system and the phones connected offer different options for making emergency calls. The administrator can configure a hotline or hotline after timeout or an emergency service.

Even if the activation period has not yet started or the communication system is in the failover period, emergency calls can always be made from the first two active telephones.

Prerequisites

The emergency call center is reached by dialing the CO access code (e.g., 0) and the emergency number (e.g., 112). The destination number for emergency calls must therefore be dialed from applications together with the leading CO access code.

Basic Sequence

Case 1: Dialing the emergency call over the PSTN line

Case 2: Dialing the emergency call via an ITSP

Case 3: Special agreement with ITSP or PSTN providers

Case 4: Emergency calls with Mobile Logon (IP Mobility)

Emergency calls are initiated by a subscriber of the communication system by dialing the CO access code and the emergency number. The emergency number is passed by the communication system on to the respective provider (PSTN or ITSP).

The emergency call is issued in the local network to which the communication system connection is assigned. The following must be observed here: All subscribers who are not in the same location as the communication system

(e.g., Mobility users, CallMe users (teleworkers) or users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

Not all ITSPs support emergency calls. In this case, the LCR configuration should be used to ensure that emergency calls are routed via the PSTN.

In cases where all subscribers of the communication system are not located at one site, but are nonetheless permanently assigned to a single site without a PSTN of its own, a customized procedure for emergency signaling can be agreed upon in cooperation with the Provider. For example, depending on the caller ID of the caller, the emergency call can be routed by the provider to the appropriate local network as agreed. These agreements are made on an individual basis and not subject to any policy.

Mobile Logon (IP Mobility) means that subscribers can change their phones and take their phone numbers with them.

Emergency calls work in this case, so long as the phones are logged in at the locations of the gateways. All subscribers who are not at the site of the gateway (e.g., Mobility users, CallMe users, home workers and users with remote WAN-linked phones) should dial the emergency call via a cell phone or another land-line phone to issue the emergency call in the local area network of their site.

INFO: For multi-gateway scenarios in which the Mobile Logon feature is used, special requirements apply. The appropriate configuration is described in the section "Emergency Calls in combination with Mobile Logon".

16.4.1 Hotline after Timeout / Hotline

You can activate the Hotline function for every station. You can thus define whether the connection to the hotline destination should be established as soon as you lift the handset (hotline) or after a short delay (off-hook alarm after timeout).

Hotline after timeout

If the subscriber selects any digit during the predefined time (hotline timeout), **no** connection to the hotline destination is established.

The hotline timeout is configured centrally by the administrator and can be activated and deactivated individually for each station.

Hotline

When the hotline is activated, the subscriber has **no** way to enter a call number after picking up the handset. It is possible to dial a number before picking up the handset. On picking up the receiver, the subscriber always reaches the predefined internal or external hotline destination automatically.

If hotline destination is set for call forwarding or call forwarding-no answer (CFNA), the calling station will always be forwarded.

System-Specific Information

The administrator can configure six hotline destinations and the length of the hotline timeout (0-99 seconds). If the administrator specifies the value 0 for the hotline timeout, the hotline destination is called immediately.

Dependencies

Topic	Dependency
Do Not Disturb	A caller hears the busy tone if Do Not Disturb (DND) is active at the destination called.

16.4.1.1 How to Configure and Change the Hotline Destination

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **Intercept/Attendant/Hotline**.
4) You can enter six different hotline destinations (**Destination call number**) under **Hotline**.
5) Click on **Apply**, followed by **OK**.

16.4.1.2 How to Change the Hotline Timeout

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **System** in the menu tree.
4) Click on **Intercept/VPL/Hotline**.
5) You can change the hotline timeout (delay period in seconds) under **Hotline**.
6) Click on **Apply** followed by **OK**.

16.4.1.3 How to Configure an Off-Hook Alarm after Timeout or Hotline for a Station

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.

3) In the menu tree, click **Stations**.
4) Click **IP Clients**, for example.
5) Click **System Clients**, for example.
6) Mark the relevant station and set the **Hotline** mode field to **Off-hook alarm after timeout** or **Hotline**.
7) If you have set Hotline, you will also need to set the **number of hotline destinations** in the Hotline field.
8) Click on **Apply** followed by **OK**.

16.4.2 Trunk Release for Emergency Call

If an emergency call is made, and no CO trunk is free, a forced disconnect occurs. The emergency caller is automatically assigned the free trunk.

Trunk release works for ISDN and ITSP trunks.

If all trunks are busy, subscribers can execute an automatic or manual trunk release.

- Automatic: The Least Cost Routing (LCR) feature is active, and there is an emergency number stored in the LCR.
- Manual: the "Release trunk" feature is always active for the Attendant Console and is executed via keys or codes.

System-Specific Information

The administrator can configure as many emergency numbers as required.

To ensure that automatic trunk release occurs when all lines are busy, the emergency number must be saved in the LCR dial plan and the *Expert Mode* emergency flag must be set for it.

16.4.2.1 How to Activate and Deactivate Trunk Release for Emergency Call

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Routing**.
3) Navigate in the menu tree to **LCR** > **Dial Plan**.
4) Select one of the following options in the **Change Dial Plan** window:
   - If you want to activate the function, enable the **Emergency Call No** check box for the corresponding call number.
   - If you want to deactivate the function, clear the **Emergency Call No** check box for the corresponding call number.
5) Click on **Apply** followed by **OK**.

16.4.3 For U.S. and Canada only: E911 Emergency Call Service

The enhanced E911 emergency service transmits geographical information on the caller (stored address) in addition to the phone number when an emergency call is dispatched.

The receiving station for the emergency call does not require human intervention to determine the site of the caller.

In the USA, this feature is only activated when the emergency number 911 is dialed.

Every station number must be assigned a valid DID number with LIN (location identification number) by the administrator for the E911 emergency service. Subscriber lines that are physically close to one another are given the same LIN. The emergency call center has a database that contains all LINs and uses the transmitted LIN to identify the name and address of the party placing the emergency call.

Dependencies

Topic	Dependency
CLIP	LIN is activated by default for the U.S. However, if CLIP (Calling Line Identification Presentation) is activated for the USA, LIN is automatically disabled.

16.4.3.1 How to Edit CLIP / Lin

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations**.
4) Click **IP Clients**, for example.
5) Click on the **Edit Stations** tab.
6) Enter the 16-digit LIN for the relevant subscriber in the **CLIP/Lin** field.
7) Click on **Apply** followed by **OK**.

16.4.4 Emergency Calls in Combination with Mobile Logon

If you use the Mobile Logon feature in a multi-gateway internetwork, switching to another phone may also change the physical location. Consequently, special measures are required for the routing of emergency calls.

Description of the Algorithm for Dialing an Emergency Number

When a subscriber dials an emergency number (ID in the LCR), an algorithm checks whether or not an emergency number has been configured for the

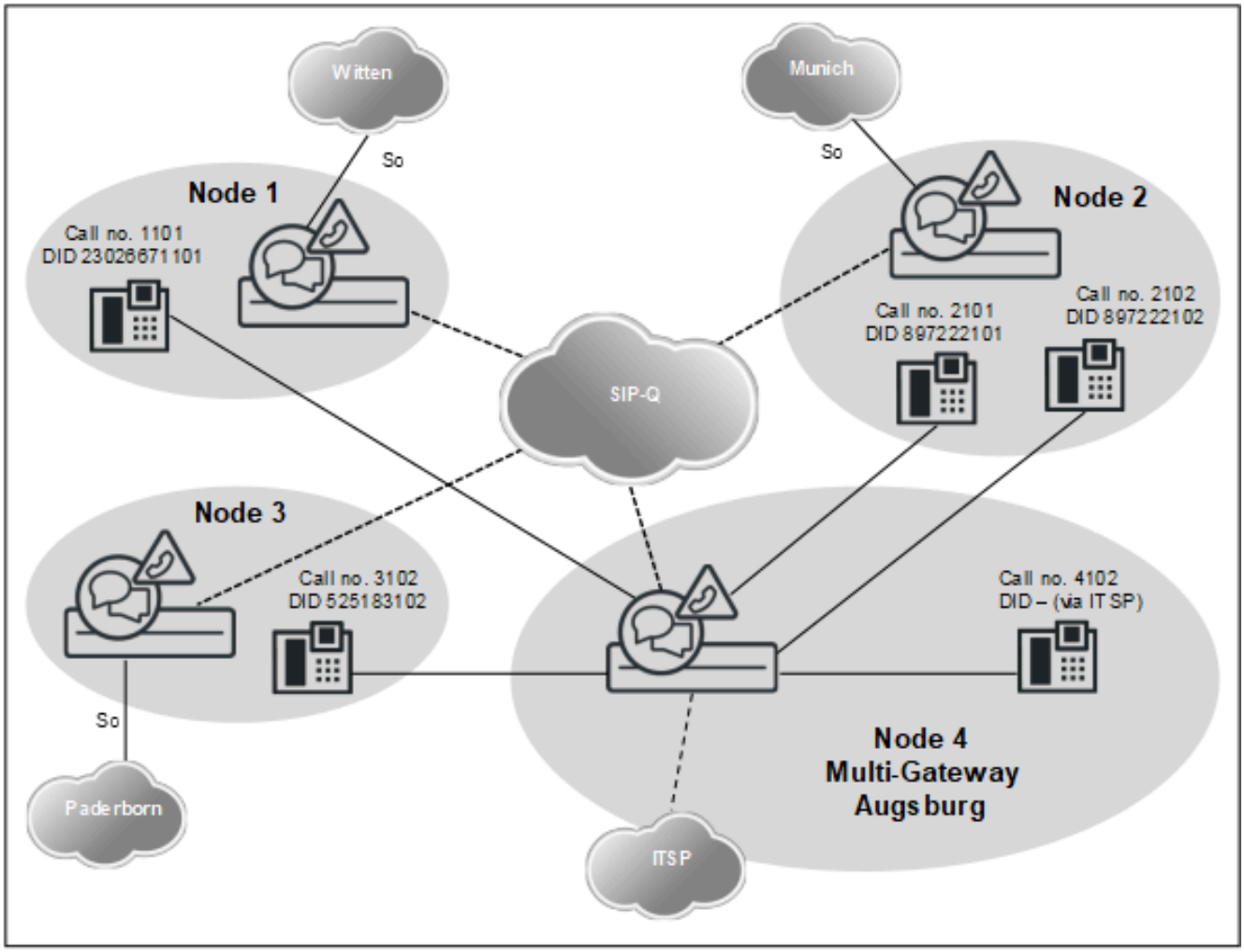
telephone. This is then used to produce a derived call number, which is used to route the call via the correct gateway in the internetwork.

Every number marked as an emergency number in the dial plan also features a reference to an entry in the route table. Every entry in the route table that is associated with an emergency number must be assigned a "low" class of service (COS). A low class of service means that every subscriber is authorized to call an emergency number.

16.4.4.1 Configuring the Emergency Scenario

The configuration of the emergency scenario shows which steps must be performed to set up emergency calling for a multi-gateway internetwork.

Handling of Emergency Numbers



Mobile Logon is supported only within a node, i.e., location changes - and thus the special requirements for emergency calls - are only relevant for phones operated on the multi-gateway node (4). In general, all affected phones are logged in at node 4, but are physically located at different sites.

- In all affected phones, one entry is required for emergency calling (connection portion of the canonical phone number of the location node + seizure code for emergency route)
- The LCR entry (node_4local) in the following table is only required if phones are physically present at node 4 (multi-gateway). It is also preceded by the location number which, however, is incomplete here (only country code). The prerequisite for this is an ITSP access to node 4, which supports emergency calls into the local network.
- On dialing at the telephone, an LCR rule marked with an emergency flag (e.g., 0C11x) is taken.
- The emergency number that is stored in the phone (and transmitted to the system at logon) is compared with the location data of the system (country code, area code, PABX number).

  If different, a "long" emergency number is formed:

  – Removal of the access code: 0112 -> 112
  – Insertion of <LDAP seizure code><international prefix><programmed emergency number>: e.g., 112 -> 0 00 49897220 112
- The "long" emergency number is routed through the LCR, either directly to the local CO (central office) using specific LCR rules or via tie lines to the respective partner node and from there into the CO.

INFO: Since the complete location number of the local node is not entered precisely in the telephone, a suitable LCR rule must also be entered for the local emergency call at the multi-gateway location.

Setting up the Location Data for Node 4

Routing parameters

Node 4, telephones

Overview of Entries Relevant for Emergency Calls in the LCR for Node 4

Node 4	Gateway Node
G.-Location Country	49
G.-Location Local Network	
G.-Location System	
International Prefix	00
National Prefix	0
LDAP seizure code	0

Route	No. and type, outgoing	RNR type
Networking	National	Int/DID

Networking Route	
CO code (2nd. trunk code)	0

Location Witten	
Call Number	1101
Emergency Number	4923026670

Location Munich	
Call Number	2101
Emergency Number	49897220

Location Paderborn	
Call Number	3102
Emergency Number	49525180

Location Augsburg	
Call Number	4102
Emergency Number	490

Dial Plan			Route table			Dial Rule		
Name	Dialed digits	Emergency operation	Route	Dedicated Gateway	Gateway ID	Dial Rule	Procedure	Type
Emergency calls [5]	0C112	X	Networking	Multi-Gateway	1	E1A	Corp. Network	Unknown
Emergency calls [5]	0C0110	X						
CO	0CZ							
Emergency_calls_to1	0C00492302667-0-11X	X	Networking	Mandatory	1	E3A	Corp. Network	Unknown
Emergency_calls_to2	0C004989722-0-11X	X			2			
Emergency_calls_to3	0C004952518-0-11X	X			3			
Emergency_calls_4local [6]	0C0049-0-11X	X	ITSP	no		E4A	Main network supplier	Unknown

16.4.5 E112 Emergency Call Service for Europe

The enhanced E112 emergency service transmits geographical information of the caller (stored address) in addition to the phone number when an emergency call is dispatched.

The geographical information is transmitted in a standardized XML document. The definition of the contents of this document depends on the country and ITSP. Thus you have to enter only the required subset of data you received from your ITSP (e.g. in Switzerland only the NAM field is used).

5 With the above rules in this example, only the emergency situation will be detected, but no routing will occur. The derived "long" emergency number is used to route the emergency call.

6 Since stations are physically connected at the multi-gateway location, a separate LCR rule must be entered for the local emergency call access (via the ITSP route).

The feature is activated through configuration of emergency numbers in LCR and defining appropriate location information.

16.4.5.1 How to add ITSP-Loc ID to a station

Prerequisites

You are logged into the WBM with the **Expert** profile

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Voice Gateway**.
3) In the menu tree, click **ITSP Loc-ID Settings**.
4) Fill the **Loc-ID Name** parameter (mandatory) and the parameter(s) defined for location information you received from your ITSP (e.g. in Switzerland only the NAM field is used).
5) Click on **Apply** followed by **OK**.

   An index id is assigned automatically to the **ITSP Loc-ID**.
6) In the navigation tree, click on **Telephony** > **Stations**.
7) In the menu tree, click **Stations**.
8) Click **IP Clients**, for example.
9) Click on the **Edit Stations** tab.
10) Enter the relevant index id of the to ITSP Loc-ID field.
11) Cick on **Apply** followed by **OK**.

16.5 Call Admission Control

Using the Call Admission Control (CAC) feature, the used bandwidth can be restricted by limiting the number of calls.

The communication system offers three ways to influence the required bandwidth:

- Limiting the number of simultaneous calls via an ITSP
- Restricting the bandwidth requirements for gateway calls
- Limiting the number of calls in network scenarios

16.5.1 Limiting the Number of Simultaneous Calls via an ITSP

The maximum number of calls that can be conducted via an ITSP can be restricted by configuring the available upload bandwidth. By reducing the number of these calls (Internet calls), the bandwidth requirements can be reduced further.

The settings for this can be made in the **Network/Internet** and **Central Telephony** wizards.

The number of possible calls via an ITSP can be viewed in **Expert mode** under **Telephony** > **Voice Gateway** > **SIP Parameters**.

Internet calls are:

- ITSP calls
- myPortal@work calls
- Device@Home calls (SIP@Home calls ,HFA@Home calls)
- Unify Phone calls

Only LAN myPortal@work and pure WebRTC calls do not reserve bandwidth because payload is direct.

When configuring the internet bandwidth and limiting the number of simultaneous calls via an ITSP, please note that some of the scenarios above occupy internet bandwidth outside of trunk contexts (myPortal@work, device@home, Unify Phone when using direct payload). In this case, the configured limit of calls for trunks may temporarily not be available.

16.5.2 Restricting the bandwidth requirements for gateway calls

By configuring the codecs allowed for Gateway calls, the bandwidth requirements can be influenced.

If only compressed codecs are set, the bandwidth requirement is lower. When using mixed codecs the prioritization of the uncompressed codecs can be reduced so that they are used less frequently.

The corresponding settings for this are made in **Expert mode** under **Telephony** > **Voice Gateway** > **Edit Codec Parameters**.

16.5.3 Limiting the Number of Calls in Networking Scenarios

The communication system offers two options for controlling bandwidth in networking scenarios.

Limitation by restricting the number of lines to other network nodes

Limitation of bandwidth through specific codec selection

By assigning a specific number of lines to other network nodes, an upper limit can be set on the number of simultaneous calls possible from and to these nodes.

The available bandwidth can be defined by configuring the codecs used from and to the partner (destination IP address).

The corresponding settings for this are made in **Expert mode** under **Telephony** > **Voice Gateway** > **Add Destination Codec Parameters**.

16.6 Tenant system

From an organizational point of view, the total capacity of the communication system can be split across a maximum of six subsystems. This makes it possible for several companies to share one communication system.

The tenant system feature is implemented using existing features. This means that it is not necessary for users to explicitly configure subsystems.

Users can control allowed and denied connections between individual stations and trunks via traffic restriction groups (CON groups).

Features in tenant service include:

- Intercept
- PABX number
- Caller list
- Override
- DISA
- Speaker call
- Call detail recording
- Hotline destinations
- Text messages, advisory messages
- Internal calls
- Internal Directory
- Customer Database Printout
- Night service
- Park slot
- Traffic Restriction Groups
- Voicemail
- Toll restriction

The communication system can be used as a tenant system, which allows it to be used simultaneously by several customers. All features have the same functionality for all users.

However, certain resources must be divided among the tenants (customers). They can be assigned to one, several, or all tenants. The resources to be divided are:

- Station
- Routes
- Attendant Console
- Intercept station
- Announcement devices, voicemail
- Traffic Restriction Groups
- Door Opener
- DISA trunks

Traffic restriction groups determine the ability of tenants to access each other.

Separate hotline destinations can be configured for each tenant.

Dependencies

Topic	Dependencies
CDRC	Only one CDRC exists for all tenants.
Internal calls	Internal calls are possible between stations in "different" tenant systems if allowed by the traffic restriction groups.
LCR	Prime Line can be configured only for the entire system.
Customer Database Printout	The database can only be printed for the entire system.
Internal Directory	The internal directory displays the names of all stations and speed-dialing numbers in the system.

Topic	Dependencies
Attendant	It is not possible to transfer undialed trunks.
Intercept	An intercept can be configured only for the entire system.

16.6.1 System Speed Dialing in Tenant Systems

System speed dialing in tenant systems enables the selection of specific speed-dialing destinations, depending on the internal traffic restriction (ITR) groups. To do this, a range of speed-dialing destinations can be assigned to the appropriate traffic restriction groups using the WBM.

Dependencies

Topic	Dependencies
External station numbers	Speed-dial destinations can contain external station numbers only.
	The external station number must include the trunk group or seizure code.
SSD names	You can assign a name to each speed-dialing destination.
Entrance Telephone (Door Opener)	The entrance telephone cannot dial speed-dial numbers.
ITR groups	You cannot assign more than one speed-dial number range for the same ITR group.

17 Attendants

OpenScape Business provides attendant functions for every use case (e.g., AutoAttendants, phone- and PC-based attendants).

Overview of Available Attendants

	Can be used for	Hardware	License
AutoAttendants			
Company AutoAttendant (UC Smart)	UC Smart	OpenScape Business X OpenScape Business S	Required
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/X5/X8 with UC Booster Card or UC Booster Server OpenScape Business S	Required
Phone-based attendants			
OpenStage Attendant			
PC-based Attendants			
OpenScape Business Attendant	UC Smart	PC and phone, UP_{0E}	Required
- OpenScape Business BLF	UC Smart	IP-based	
myAttendant	UC Suite	OpenScape Business X3/X5/X8 with UC Booster Card or UC Booster Server OpenScape Business S	Required

17.1 AutoAttendant

The AutoAttendant, together with the voicemail, provides an integrated automated Attendant service and a message store, e.g., for the company headquarters. The AutoAttendant plays a greeting to callers. During or after this announcement, the caller can be routed to an extension or mailbox automatically or by entering digits.

A wide range of functions for specific switching are available for this purpose, together with the corresponding prompts, e.g., "Press 1 for service, 2 for Sales, etc". After entering the desired digit, the caller is then automatically connected with the Sales or Service staff.

The Company AutoAttendant is not assigned to any internal call number, but to a central instance. Multiple Company AutoAttendants or mailboxes can thus be assigned to one extension. This makes it possible for the user to individually redirect to the appropriate Company AutoAttendant. Depending on the redirection, the caller hears either the announcement of the personal mailbox or the central company announcement. It is, however, also possible to play back individual announcements via the Company AutoAttendant, regardless of the personal mailbox.

Function Overview

- Intercept after announcement to a configured destination
- Status-based announcements - depending on the status of the extension (free or busy), different announcements can be played.
- Different day/night announcements (switching occurs either manually or automatically)
- Central calendar control via the automatic night service
- Suffix-dialing of any call number up to a configured length (can be deactivated)
- Speed dialing (= direct dialing external location) to configured destinations (any call number or mailbox)

  A total of 4 lists with a total of 10 destinations and one intercept destination are possible. The active list is determined by the selected greeting.
- Suffix-dialing of any call number up to a configured length. Suffix-dialing can also be disabled to prevent toll fraud.
- Multistep AutoAttendant

  AutoAttendant mailboxes can be configured as speed dial destinations (Manual 1 to 4, day/night). This allows for a concatenation of mailboxes.

  In this case, the Company AutoAttendant acts in the same manner as for call forwarding, i.e., the call is forwarded from one concatenated mailbox to the next, and each time the respective announcement is played. In total, up to 100 AutoAttendant mailboxes are available.
- Speed dialing

  Announcements can be disabled to guarantee fast switching.
- Announcement Prior to Answer with Parallel Signaling (without Speed Dialing)

  While the greeting is being played to the caller, the call is also simultaneously signaled to the subscriber acoustically (and visually). If the subscriber picks up the call, the announcement is interrupted, and the subscriber is connected to the caller. If the subscriber does not pick up the call, the announcement is played in a loop until the caller hangs up or is routed through the call management.
- Busy tone detection
- Forwarding of fax calls (automatic fax tone recognition) to a preconfigured Fax destination.
- Automatic recall

  In the case of a recall (except for fax calls), the caller is forwarded to the connected mailbox, if such a mailbox is available and message recording has been enabled.

NOTICE: I order to enable an automatic intercept from the voicemail system to the attendant console, the attendant code must be entered internally (default 9, USA 0).

NOTICE: AutoAttendant mailboxes can only be administered from a telephone (TUI). This is why the password for the AutoAttendant mailbox should differ from the password for the personal mailbox of the phone!

Use Cases

- Example 1: **Independent standby or emergency services announcements**

  Outside business hours, the customer is redirected to the AutoAttendant (e.g., via the night service). The AutoAttendant connects to the respective on-duty service technician on request and offers the option of leaving a message in a central mailbox. In this case, one announcement enables redirection to the various mobile phone numbers of the service technician.
- Example 2: **Different Sunday services for medical practices**

  It is now no longer necessary to record the currently applicable Sunday service on the answering machine and to replace the AB cartridge. The customer configures as many AutoAttendants as the number of available representatives. The AutoAttendants are recorded once and activated each weekend with a redirection (night service) to the appropriate AutoAttendant. Here the situation is reversed: several different announcements lead to the same mailbox.

17.1.1 Company AutoAttendant (UC Smart)

The Company AutoAttendant (UC Smart) is the Attendant Console of the UC solution UC Smart. It can be used as a personal AutoAttendent and as a central AutoAttendant. The initial setup is performed via the WBM, after which it can subsequently be controlled and configured over the telephone.

The Company AutoAttendant (UC Smart) can be operated in two modes:

- **Personal AutoAttendant**

  The personal AutoAttendant is assigned to a subscriber or group and responds to the call number of the originally called, redirecting subscriber or group (e.g., `12345678-100`).

  The personal AutoAttendant is reached via the "voicemail" hunt group (default call number: 351). Operation occurs via SmartVM ports (EVM ports) of type "PhoneMail", which must all be assigned to this hunt group.

  Parallel operation with UC Suite is not possible.
- **Central AutoAttendant**

  The central AutoAttendant is used as a central attendant console and responds to its own call number (e.g., `12345678-0`). Regardless of whether a direct call to the AutoAttendant or a diverted call is involved, the behavior is always the same.

  The central AutoAttendant is reached via one or more of its own hunt groups (default call number: 352). Operation occurs via SmartVM ports (EVM ports) of type "Standard", which can be assigned to one or more hunt groups (max. 100).

  By default, a Company AutoAttendant (group index 3) is configured with 2 SmartVM ports. The names and types of ports can be changed with the **Central Telephony** > **SmartVM** wizard (see also How to Configure the Voicemail Box (SmartVM)).

  The speed dial list and the greetings upload be changed in Expert mode under **Telephony** > **Auxiliary Equipment** > **SmartVM** (see also How to

Load, Save and Delete Individual Greetings). Additional (max. 99) Company AutoAttendants (UC Smart) can be likewise set up and activated.

Parallel operation with UC Suite is possible.

The Company AutoAttendant (UC Smart) requires a license (Company AutoAttendant license). If no license is present, the "rules" of the Company AutoAttendant are ignored, and calls are forwarded to the central intercept position.

17.1.1.1 How to Configure an Established Company AutoAttendant

As an example, for calls during the day, an announcement before answering is to be set up with a recording option (e.g., mailbox 100). During the night, after the appropriate announcement, calls are to be intercepted and sent directly the night voicemail box with a recording option (also mailbox 100).

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

By default, during day and night service, an intercept to the intercept position occurs after the announcement.

By default, the speed-dial function and suffix-dialing are not enabled.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
3) In the menu tree, click on **Auxiliary Equipment** > **SmartVM**.
4) Click on **AutoAttendant** in the menu tree.
5) Clear the **Intercept after announcem.** check box in the row of the desired AutoAttendant (e.g., `352`) to enable the entry of speed dial digits during the greeting.
6) Select the **no suffix-dialing** check box. As a result, only the entry of speed dial digits will be possible (i.e., no internal call numbers can be entered).
7) Click on **Apply** followed by **OK**.
8) Click in the menu tree on **AutoAttendant** and then on the entry for the desired AutoAttendant (e.g., `352`).
9) Click on the **Edit Speed Dial/Intercept Dest. Day** tab.
10) Select the station for the intercept position (e.g., station 100) from the **Select** drop-down list in the **Speed dial 0** row and then select the entry **Mailbox** in the **Type** drop down list.
11) Select the station for the intercept position (e.g., station 100) from the **Select** drop-down list in the **Intercept** row.
12) Click on **Apply** followed by **OK**.
13) Click on the **Edit Speed Dial/Intercept Dest. Night** tab.
14) Select the station for the intercept position (e.g., station 100) from the **Select** drop-down list in the **Intercept** row and then select the entry **Mailbox** in the **Type** drop down list.
15) Click on **Apply** followed by **OK**.

16) Click on **SmartVM** in the menu tree.
17) To avoid a two-fold greeting for the Intercept voicemail box, select the entry **None** from the **Greeting** drop-down list in the row of the intercept position (e.g., station 100). This causes the signal tone for recording to immediately follow the greeting of the Company AutoAttendant.
18) The greeting of the Company AutoAttendant can be changed through a telephone or via the **Expert Mode** > **Maintenance** > **SmartVM** (see Configuring the Voicemail Box (SmartVM)).

17.1.1.2 How to Set up a New Company AutoAttendant

Prerequisites

You are logged into the WBM with the **Expert** profile.

UC Smart has been activated.

Required licenses

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) First, configure the hunt group:
   a) In the navigation tree, click **Telephony** > **Incoming Calls**.
   b) Click **Incoming Calls** > **Groups/Hunt groups** in the menu tree.
   c) Click on the **Add Group** tab.
   d) Enter the station number of the new AutoAttendant (e.g., `353`) in the **Station Number** field.
   e) Enter the DID number of the new AutoAttendant in the **Direct inward dialing number** field (e.g., `353`).

      INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

   f) Enter the name of the new AutoAttendant in the **Name** field (e.g., `AutoAttendant 353`).
   g) Select **Cyclical hunt group** from the **Type** drop-down list.
   h) In the **Group member** area, select the desired AutoAttendant port (e.g., **745 SmartVM 7**) from the Call No drop-down list.
   i) Click on **Apply** followed by **OK**.
   j) To add another AutoAttendant port of the hunt group, click in the menu tree under **Groups/Hunt groups** on the desired AutoAttendant and then on the **Add member** tab. Then select another AutoAttendant port there (e.g., **746 SmartVM 8**) under **Station Number**.
   k) Click on **Apply** followed by **OK**.

3) Configure the AutoAttendant mailbox:
   a) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
   b) Click on **Auxiliary Equipment** > **SmartVM** in the menu tree.
   c) Click on **AutoAttendant** in the menu tree.
   d) Set the two check boxes as required in the row of the desired AutoAttendant (e.g., `353`):

      Intercept after announcem.: When activated, the caller can enter a speed dial digit for a switching option during the greeting.

      No suffix-dialing: If enabled, only speed-dial digits and no internal call numbers can be entered.
   e) Click on **Apply** followed by **OK**.
   f) Click on **SmartVM** in the menu tree.
   g) Click on the
   h) On the **Edit SmartVM Mailboxes** tab, select the desired greeting under **Greeting** in the row of the desired AutoAttendant.
   i) Select the **AutoAttendant** check box in the row of the desired AutoAttendant.
   j) Click on **Apply** followed by **OK**.
4) Configure the switching options (e.g., "0" to connect and "1" for an announcement):
   a) Click in the menu tree on **SmartVM** and then on **AutoAttendant**.
   b) Click in the menu tree under **AutoAttendant** on the entry of the desired AutoAttendant (e.g., `352`).
   c) Click on the **Edit Speed Dial/Intercept Dest. Day** tab.
   d) In the **Speed dial 0** row, enter the phone number to which calls should be connected under **Call number** and select the entry **Call no.** in the **Type** drop-down list.
   e) Select the station for the intercept position (e.g., station 100) from the **Select** drop-down list in the **Speed dial 1** row and then select the entry **Mailbox** in the **Type** drop down list.
   f) Select the Company AutoAttendant (e.g., `353`) from the **Select** drop-down list in the **Intercept** row.
   g) Click on **Apply** followed by **OK**.
   h) If the flag **no suffix-dialing** is disabled, internal numbers can also be dialed during the greeting. To prevent toll fraud, the **Call number length delimitation** should be checked and restricted so that no external phone numbers can be dialed (see **Expert Mode** > **Telephony** > **SmartVM** > **Edit SmartVM parameters**).

17.1.2 Company AutoAttendant (UC Suite)

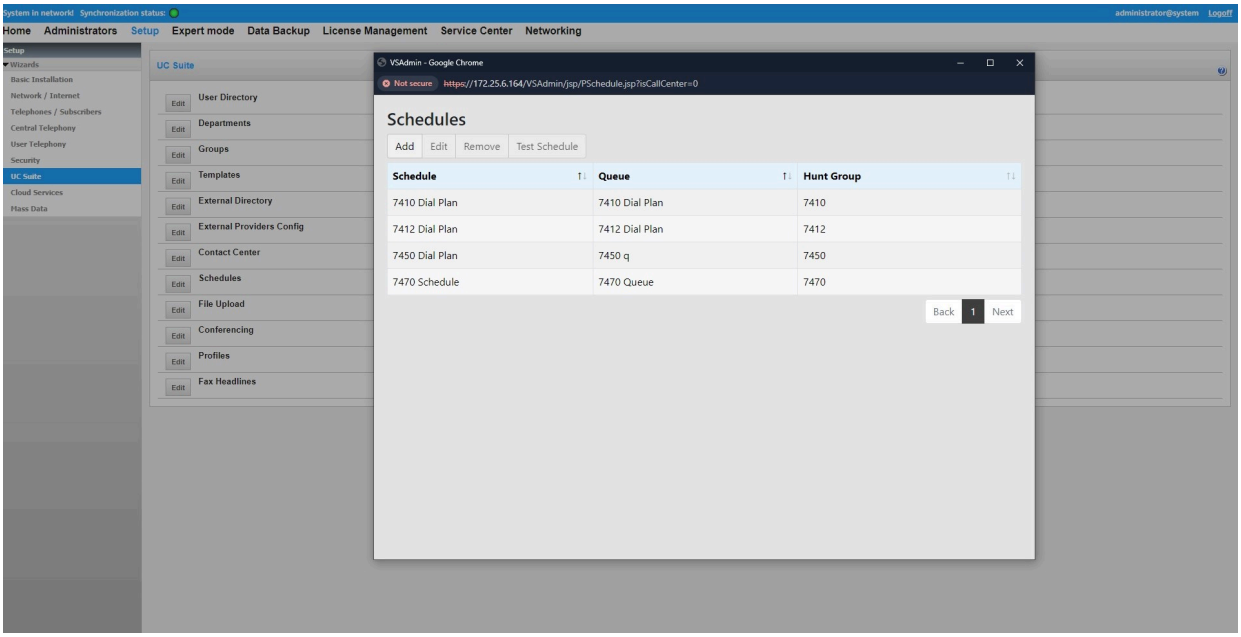
The central Company AutoAttendant (UC Suite) is an attendant console which can only be configured by the administrator. To facilitate the installation and setup, there are five templates that can be customized by the administrator.

The administrator can configure the Company AutoAttendant (UC Suite) on the basis of rules and schedules. Schedules also make it possible to offer advanced selection options such as dialing by name, for example.

17.1.2.1 Schedules

This schedule and the rules contained in it (Call Control Vectors or CCVs) define how incoming calls are to be handled on specific dates and at specific times.

For example, on work days, separate rules may be defined for the morning shift (from 6:00 to 14:00 hours), the afternoon shift (14:00 to 22:00 hours) and the night shift (from 22:00 to 06:00 hours). Similarly, a weekend rule can defined for the weekends. For each of these rules, you can define whether an announcement is to be played, for example, and/or the destination to which the calls are to be forwarded.



A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects and can be saved under a user-defined name upon completion.

Saved rules can be assigned to one or more schedules as a default rule (default CCV) or an exception rule (exception CCV). They can be opened, edited and saved again at any time by using the rule editor.

After a schedule has been assigned a default rule (default CCV), this schedule can be saved under a user-defined name. A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules.

Rule Editor (CCV Editor)

The Rule Editor is used to create rules from predefined CCV objects. The arrangement of the CCV objects and their properties determine how incoming calls are to be handled.

NOTICE: A rule has an upper limit of 500 CCV objects.

The following predefined CCV objects are available:

INFO: For all of the named CCV objects, the two general properties listed below also apply:

Description: Optional entry to describe the CCV object, e.g., Greeting.

Process digit: specification of the digit(s) required without blanks, commas or other characters. The specification refers to the preceding CCV object. If 9 was specified there under Accepted Digits, then 9 must also be entered here.

- **Play Message**

  Causes the desired message to be played. Any audio file present in the UC Suite can be selected. In addition, a new audio file can be imported into the UC Suite or a new announcement can be recorded and then imported as an audio file into the UC Suite.

  The playback of the announcement seizes one respective Media Stream channel.

  Properties:

  – **File Name**: Selection of an announcement (audio file in WAV format)
  – **Interrupt Digits**: specification of a key or key combination on the dial pad with which callers can stop the playback of an announcement.
  – **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.
- **Disconnect Caller**

  Causes the call to be disconnected.

  After this CCV object, no further CCV object may be inserted.
- **Go to CCV**

  Causes a loop to another CCV object

  Property:

  – **Target CCV**: Selection of the CCV object

- **Process after digits**

  Causes the next CCV object(s) to be executed, depending on the digits specified there (process digit).

  Properties:

  – **File Name**: Selection of one or more announcements (audio file in WAV format)
  – **Playlist**: List of selected announcements (audio file in WAV format) in the order in which they are played
  – **Digits Timeout**: Time, in seconds, for which the communication system waits for the input of digits.

    If the required digits are not entered fully within the specified time, the message (announcement) is played again.
  – **Link To**: List of digits with destination.

    The digits and destinations can be added, edited and removed.
  – **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.

  The contents of the Playlist are presented in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.
- **Single Step Transfer**

  This function depends on the **Normal Attendant Console SST** setting (WBM, **Expert mode**: **Applications** > **OpenScape Business UC Suite** > **Server** > **General Settings**):

  – **Normal Attendant Console SST** enabled (default setting; not for U.S.): Causes the call to be transferred, regardless of whether the destination is free, busy or unavailable.

    INFO: For stations with call waiting rejection enabled, the call is switched through only if the destination station is free. No call waiting on busy occurs.

  – **Normal Attendant Console SST** disabled (default setting, only for U.S.): Causes the call to be transferred if the destination is free.

    If the destination is busy and call waiting rejection is disabled, or if the destination is unavailable, an announcement is played back to the caller. The caller can then optionally choose to leave a message in the

voicemail box of the called subscriber or select the call number of another destination.

If the destination is busy and call waiting rejection is enabled, the call is not switched through.

After this CCV object, no further CCV object may be inserted.

Property:

– **Target Extension**: specification of the internal call number or external DID extension with the number of the CO trunk. Blanks, commas and other characters are not allowed.

The call number of the target extension is displayed in the CCV object.

NOTICE: After Single-Step-Transfer, the system disconnects the call after ringing for 5 minutes.

- **Record In Mailbox**

  Causes the call to be sent to the desired voicemail box of a subscriber or a voicemail group

  After this CCV object, no further CCV object may be inserted.

  Property:

  – **User Mailbox**: specifies the station number of the voicemail box of a subscriber or voicemail group

  The station number and the name of the voicemail box or voicemail group are shown in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

- **Supervised Transfer(also called screened transfer)**

  Causes the call to be transferred to an internal destination. During the transfer, Music on Hold (MOH of UC Suite) is played back to the caller.

  In contrast to the single-step transfer CCV object, two further CCV objects must be inserted here. This is because we now need to define how the communication system should behave if the call destination is busy or does not answer the call. Usually, an announcement is played to the caller in such cases.

  Properties:

  – **Target Extension**: Specification of the internal phone number.

    Only internal call numbers are supported in the own node. Forwarding to external destinations, virtual stations, additional AutoAttendants, UCD (incl. Contact Center) as well as external CallMe destinations is not allowed! For these scenarios, the SST (single-step transfer) should be used.

  – **Ring Time Out (SEC.)**: Time, in seconds, within which the call must be accepted.

    If the call is not answered within the specified time, it is returned to the communication system, and the next CCV object is used.

    INFO: The time specified here must be shorter than the time configured for call forwarding (the default setting for

call forwarding = 15 seconds). See How to Configure Call Forwarding.

– **Pull back call if destination device is forwarded / deflected**: Option (only applicable for internal call number.)

  If this option is enabled, the call destination is first checked, and if a forwarding destination or deflection has been set for it, the call is returned to communication system, and the next CCV object is used.

– **Check Presence status when transferring call**: Option

  If this option is enabled, the presence status of the call destination is checked, and if this status is any presence status other than Office, the call is returned to communication system, and the next CCV object is used.

  NOTICE: If an incoming call comes from a suppressed/ unknown number and the call is answered by UC Suite AutoAttendant and transferred using Supervised Transfer, the displayed caller number will be the UC Suite number.

- **Dial By Name**

  Causes the caller to be prompted to enter the first three letters of the desired subscriber's last name via the dial pad.

  If a unique subscriber name with the entered initial letters is found, a connection is established.

  If there are several subscriber names with the entered initial letters, these subscriber names are announced to the caller (max. 10 subscribers). If a subscriber has no recorded name announcement, the call number is announced instead. After selecting the desired subscriber, a connection is made.

  If none of the subscribers match the entered initial letters, the caller receives a corresponding message.

  INFO: The keys on the dialpad respond to the first press of a key. With each key pressed, the system tries to determine whether there are subscriber last names with the letter assigned to that key.

  Example: Let us assume the internal phone book has five last names with the initial letters t, u and v: Taylor, Taler, Ullrich, Vasquez and Volterra. To establish a connection with the subscriber Taylor, following keys must be pressed: 8 2 9

  After this CCV object, no further CCV object may be inserted.

  Properties:

  – **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.

    Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

- **Dial By Extension**

  Causes the caller to be prompted to enter the station number (extension) of the desired subscriber via the dial pad.

  If the caller dials the station number of a virtual station, the caller is prompted to enter another station number. A connection is then established. If the desired subscriber does not respond, the call is accepted by his or her voicemail box.

  After this CCV object, no further CCV object may be inserted.

  Properties:

  – **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.

    Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions in the network for which the phone number is entered in the internal directory are supported here.

- **Set language**

  Selects the language for each standard announcement based on the phone number of the caller. It should be noted that only standard announcements (i.e., system announcements) and no personal greetings are taken into account here.

  For example, it is possible to have German announcements played back to callers with the country code +49 and French announcements for callers with the country code +33.

  Properties:

  – **Default language**: Drop-down list to select a language.

    The language selected here is used for all phone numbers for which no specific language was defined.

  – **Pattern**: Specifies the phone numbers to which a particular language is to be assigned.

    The following placeholders can be used * = any digit, ? = any digit.

  – **Language**: Drop-down list to select the language to be assigned to the relevant phone numbers (matching **Pattern**).

  A language can be assigned to any number of different phone numbers (matching **Pattern**).

- **CLI Routing**

  Causes the forwarding of a call to one or more sequential CCV objects based on the caller's number.

  For example, it is possible to first have a German announcement played back to callers with the country code +49 (CCV object **Play Message**) and then have the call forwarded to an internal phone (CCV object **Single Step Transfer**). The area code can also be used (e.g. 089 for Munich).

  In the context of UC Suite and CLI Routing, users need to consider specific scenarios, such as incoming calls from MS Teams Native SIP Trunk. If you intend to send towards OpenScape Business caller's numbers in canonical format, including country code, then you have to establish additional CLI Routing rules.

  For example, if callers from MS Teams have numbers in the format +49777555XXXX, and 777555 is the common part of these numbers, users

should create relevant CLI Routing rules that incorporate this common part (777555).

Properties:

– **Standard**: Drop-down list to select the CCV object.

  The CCV object selected here is used for all phone numbers for which no specific destination was defined.
– **Pattern**: Specifies the phone numbers to which a specific CCV object is to be assigned as the destination.

  The following placeholders can be used * = any digit, ? = any digit.
– **Description**

  Provides an explanation.

  For the **Pattern** +49 (= country code for Germany), for example, Germany can be entered.

  The text entered here will appear in the Rule Editor.
– **Target**: Drop-down list to select the CCV object that is to be assigned as a destination to the related phone numbers (matching **Pattern**).

A CCV object can be assigned as a destination to any number of different phone numbers (matching **Pattern**).

• **Branch on variable**

Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.

You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.

Properties:

– **Variable**: Selection of **Calls** or **Available agents**.

  Depending on the selected variable, the number of calls waiting in a queue or the number of available agents (including agents in wrap up time) is used as the defined condition. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to**

or greater than, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field.
- **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
- **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.

The number of available agents in a queue is affected by the following status changes of the agents:

- Login of an agent into the queue using "Anmelden/Login": --> +1
- Logout of an agent from the queue using "Abmeldung/Logout": --> -1
- Agent in the status "Break":-->-1
- Agent in the status "Available after Break":--> +1

The number of available agents in a queue is **not** affected by the following status changes of the agents:

- Agent in the status "Ringing"
- Agent in the status 'Talking'
- Agent in the status "Wrap up"
- Agent in the status "Missed Call"
- Agent in the status "Overdue"

17.1.2.1.1 How to Add an Exception in CCV

If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules, as an Exception CCV. This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules.

Between different exception types **Holiday Schedules** exception has higher priority than **Within time range** and **Within time date range** exceptions.

Similarly, **Within time range** and **Within time date range** exceptions have higher priority than **Yearly Recurrence** exception.

For the same exception type, the ones created at a later time have higher priority than the ones created earlier.

Step by Step

1) Navigate to **Expert mode > Applications > OpenScape Business UC Suite**.
2) Click on **Schedules**, select one of the available schedules and click on **Edit**.
   You can click on **Add** to create a new Schedule.
3) Click on **Add** in the **Exceptions** area.
4) Fill in the **Description** field, if you want.
5) Select the type of the exception from one of the available options:
   - **Within time range**: select a specific time, day and recurrence for the exception
   - **Within time date range**: select a specific date, time, day and recurrence for the exception
   - **Holiday Schedules**: select a specific Holiday date for the exception
   - **Yearly Recurrence**: select whether the exception will repeat every year
6) If applicable, select values for **Start Date** and **End Date**.

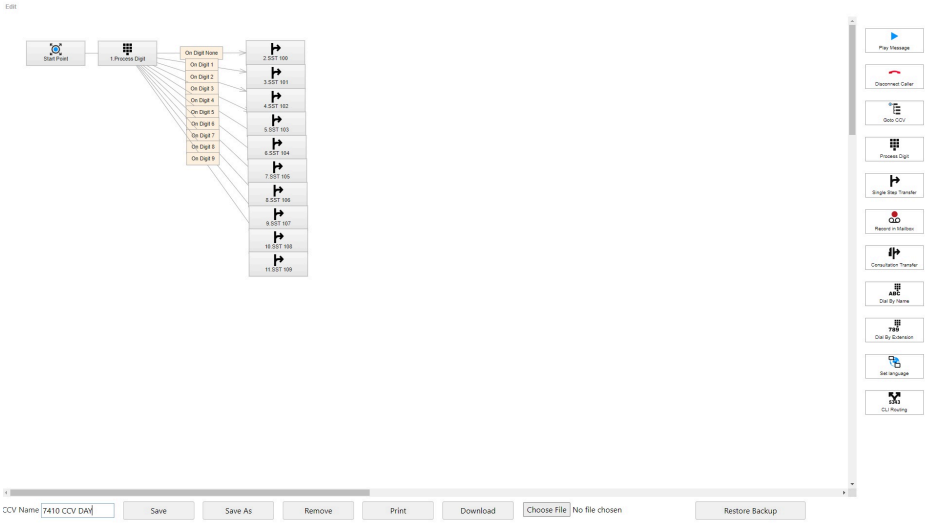
7) Select **Start Time** and **End Time** from the corresponding drop-down lists.
8) Select and click next to the days for which the exception will occur. You can also select a predefined set of days, by clicking next to **Everyday**, **Every Weekday**, **Weekends**.
9) Click on **Save**.

17.1.2.2 Templates

The following templates are predefined, standardized templates for the Company AutoAttendant (UC Suite), but can be changed as desired and adapted to specific needs.

Template 1 - 7410 CCV: Call with Switching (without Voicemail)

An announcement is played for the caller. The caller is then prompted to press a button (digit) and is connected to a subscriber. If the caller does not press any button, the call is switched to to the intercept position (default 100).



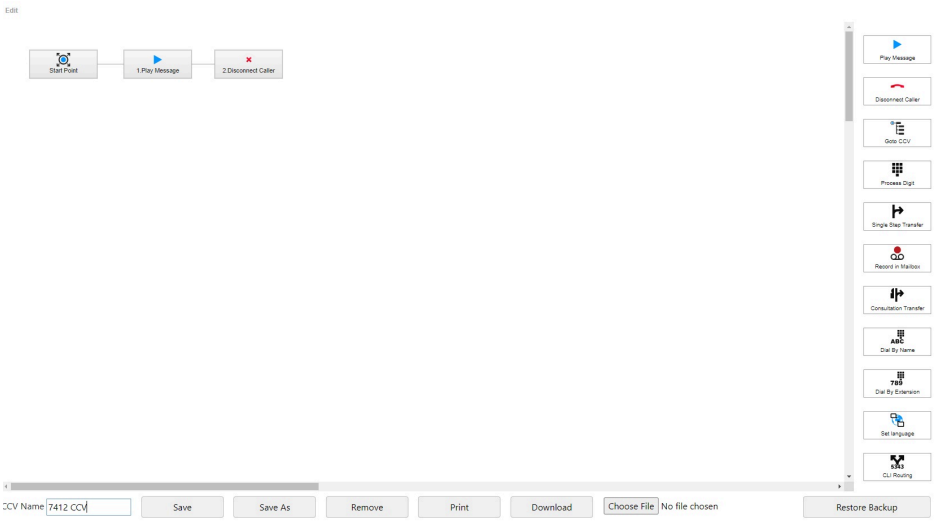
Template 2 - 7411 CCV: Announcement before Answering

An announcement is played for the caller. The call is then switched to the intercept position 100.



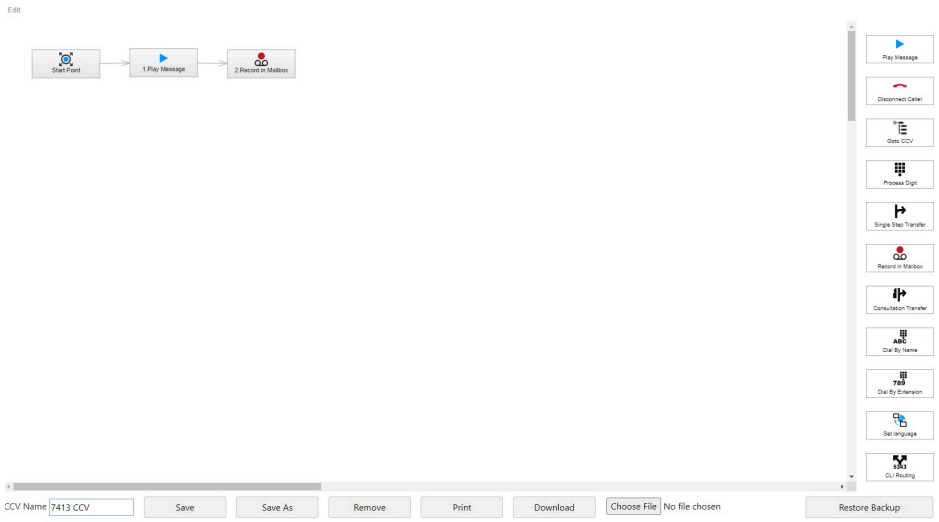
Template 3 - 7412 CCV: Call Outside Business Hours

An announcement is played for an incoming call outside business hours. The call is then disconnected.



Template 4 - 7413 CCV: Call Outside Business Hours with Call Forwarding to Voicemail

An announcement is played for an incoming call outside business hours. The caller is then prompted to optionally record and leave a message in a voicemail box.



17.2 OpenStage Attendant

Attendant functions can be performed using a specially configured OpenStage telephone. The OpenStage Attendant is also an intercept position.

Key layout

OpenStage Attendant is the destination for all incoming non-DID calls and calls for which no users could be reached (intercept calls) via the call allocation criteria. The attendant then routes these calls to the correct destination.

The following OpenStage phones can act as an Attendant:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

On OpenStage telephones configured as attendant consoles, the programmable function keys are assigned as follows:

- Night service
- Directory (phone book)
- Queued calls
- Override
- Hold
- External 1
- External 2 (not for OpenStage 40)
- Empty unassigned key (not for OpenStage 40)

17.3 OpenScape Business Attendant

The OpenScape Business Attendant provides switching functions as well as the connection of a phone book for OpenScape Business. In a network, the

OpenScape Business Attendant can be expanded to show network-wide BLF and presence information.



Main attendant functions:

- Manage waiting or accepted calls
- Data of the active call
- Parked, held calls
- Call List
- Journal for answered, missed and outbound calls
- Personal VoiceMail

Directory (phonebook) application:

- Outlook contacts
- LDAP (connection via OpenDirectory Service)
- Personal directory

BLF status:

- Free, Busy, Called, Forwarded

Presence visibility:

- Office, Meeting, Sick, Break, Out of the Office, Vacation, Lunch, Gone Home

> **NOTICE:** The "sick" presence status may not be available, depending on system settings by the administrator.

- Change the presence status for users within your own node (currently not possible for users from other nodes)

Two different "styles" are available for customizing the OpenScape Business Attendant user interface.

You can connect a maximum of eight OpenScape Business Attendants per communication system (a maximum of eight licenses per OpenScape Business X1/X3/X5/X8 and Business OpenScape Business S).

OpenScape Business Attendant is licensed via the WBM.

Technical Requirements

- Standard Windows PC
- Possible use of a Terminal Server when using HFA telephones (see Prerequisites for UC Suite PC Clientsfor the related prerequisites)
- USB interface or LAN interface, depending on the telephone used
- Screen with a resolution of min. 1024x768, optional second screen to display the second BLF
- Video card with 16-bit color depth (min. 256 colors)
- Internet access for support or updates

Operating System

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server

Support for OpenScape Business Attendant for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Supported Phones

- 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

> **NOTICE:** Regarding OpenScape DeskPhone CP 200/205/210, the name of the user is not shown for an external call.

Some of the older devices (e.g., optiPoint 410/420/500) are still supported. Please refer to the relevant release notes to see which devices have been tested and released.

Plug-and-Play Installation

The initial setup of the OpenScape Business Attendant is wizard-based. The wizard automatically opens all required configuration dialogs.

e.g.:

- Query the terminal type
- Query and check system access
- Query and check internetwork, if any
- Automatic integration of the BLF.

17.3.1 OpenScape Business BLF

The Busy Lamp Field, OpenScape Business BLF, is a separate application for displaying busy states. Optional functions include displaying and setting the presence status, and setting up the connection for the associated phone.

Technical Requirements

Main functions:

- OpenScape Business BLF is scalable and customizable
  - 10 to 350 BLF fields (user buttons), depending on the screen resolution
- Phone functions
  - Dial
  - Call answer
  - Disconnect
- Set the presence status (for own station)
- Directory (system directory)
- Call Journal

One OpenScape Business BLF license plus one UC User license are required to operate each OpenScape Business BLF.

- Standard Windows PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Screen with a resolution of min. 1024x768
- Video card with 16-bit color depth (min. 256 colors)
- LAN interface
- Standard mouse and keyboard
- Internet access for support or updates

17.3.2 Configuration Examples for OpenScape Business Attendant, OpenScape Business BLF

In the following sections you will find configuration examples for the general configuration of OpenScape Business Attendant, OpenScape Business BLF.

17.3.2.1 Scenario 1: OpenScape Business Attendant Connected to an OpenScape Business Single System

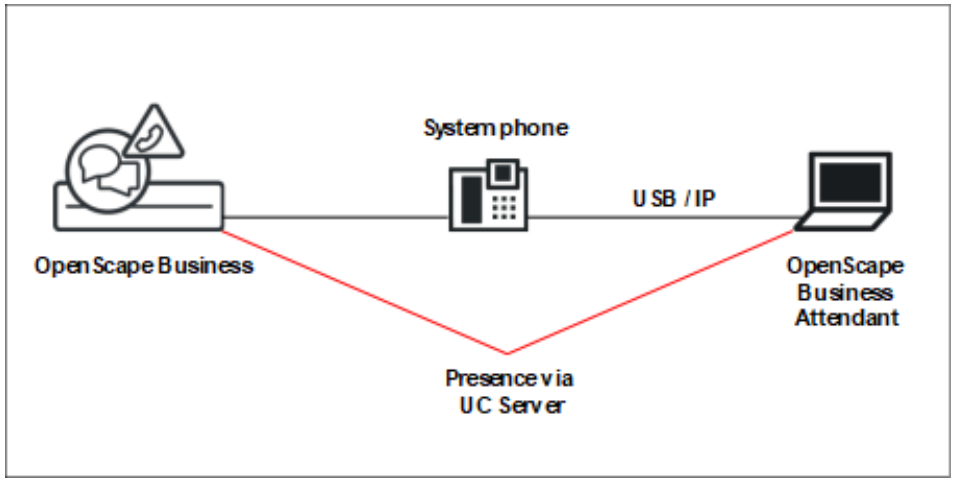
Prerequisites

The license for OpenScape Business Attendant is present.

Telephone with valid license

License for UC Smart or UC Suite for presence information (optional)

The IP address for the Web Service Interface is different for UC Smart and UC Suite. In the case of UC Smart, the WSI always runs on the communication system; for the UC Suite, by contrast, it runs on the Application Board or Application Server (see UC Smart and UC Suite). If Booster Server is in use, the IP-address of Booster Server has to be used while if OCAB is in use, the IP-address of the OCAB has to be used. Only if both components are not connected, communication system's IP must be used.



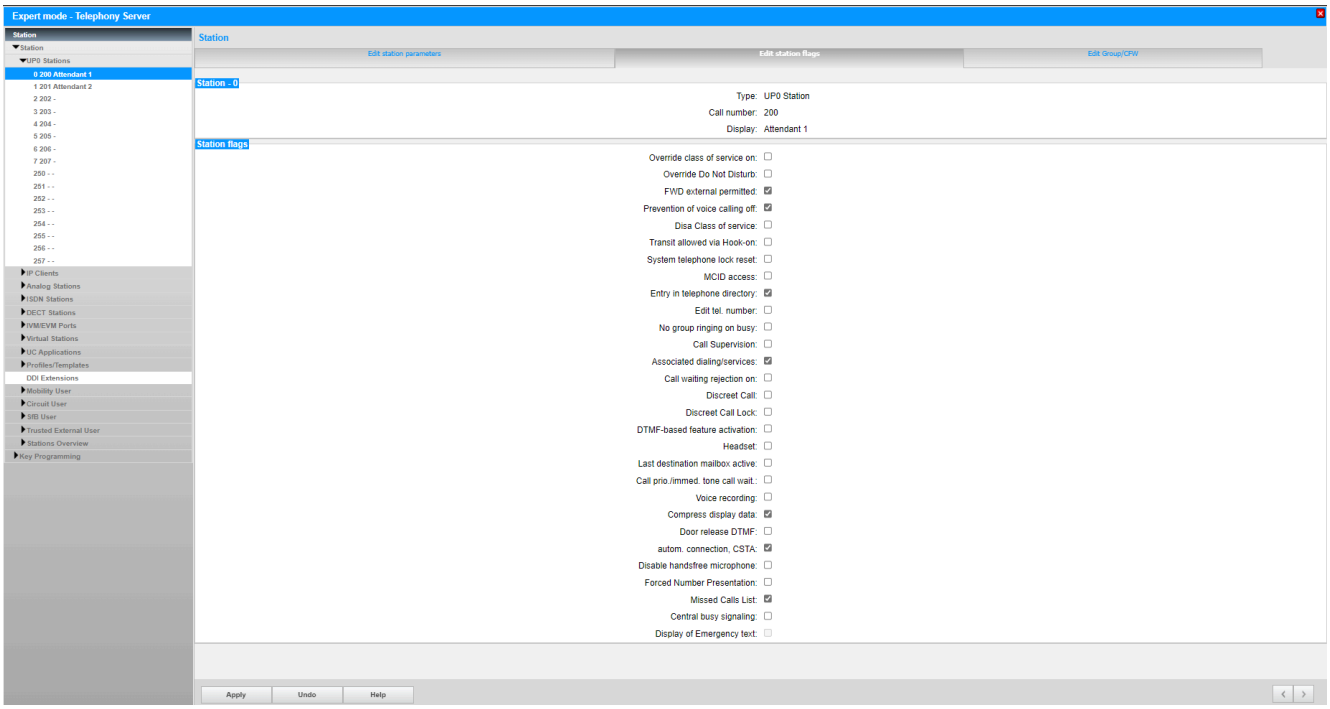
Step by Step

1) Configure a station as an attendant using the WBM or Manager E (optiPoint 500, OpenStage 30T, 40T, 60T, 80T or OpenStage 40HFA, 60HFA, 80 HFA).

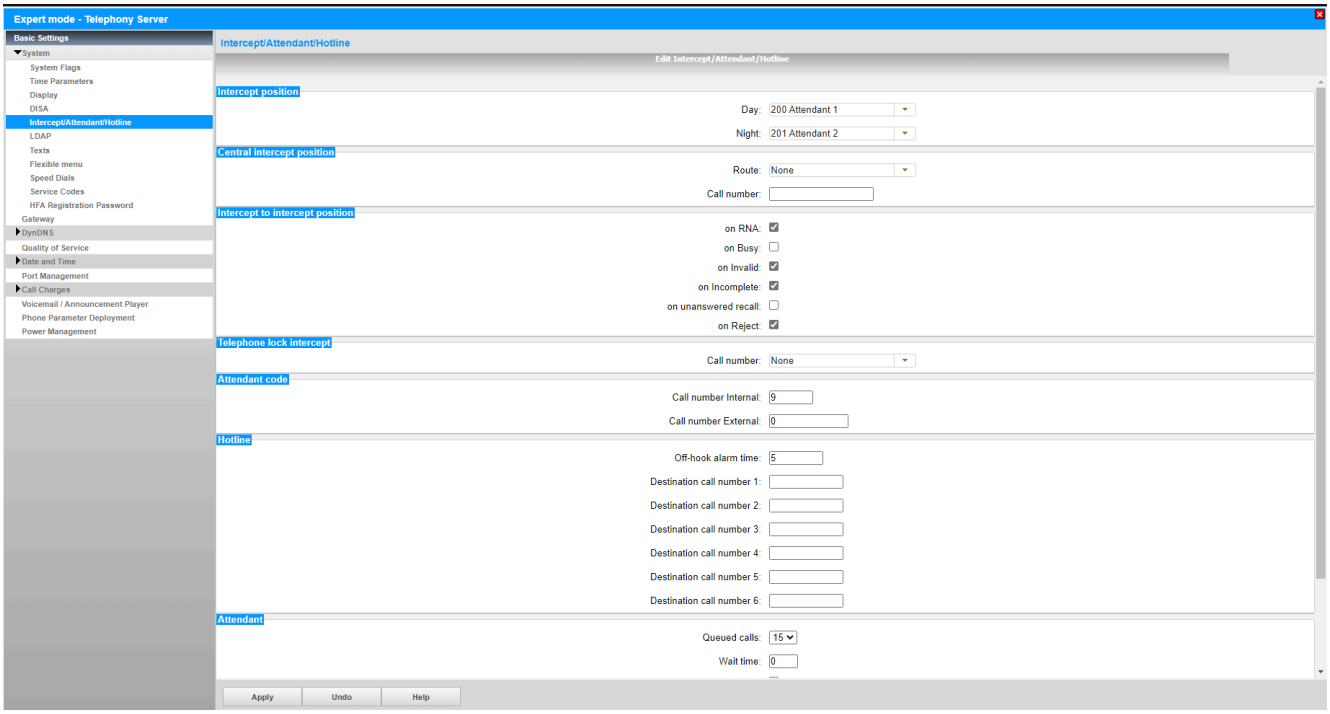
   INFO: SIP or CMI phones have not been released.

2) Configure the **Associated services** feature. This is needed for the OpenScape Business Attendant to enable and disable features for other stations.

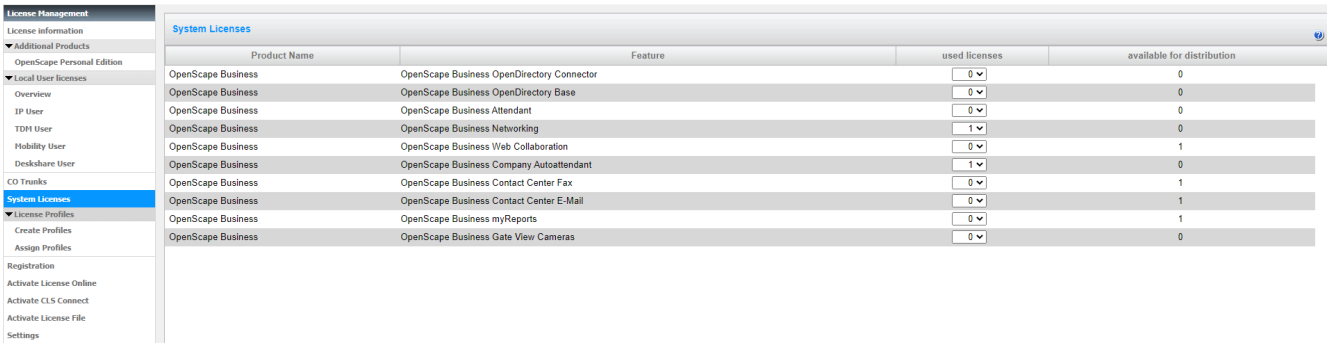
3) Activate **Override Do Not Disturb** and disable **Call waiting rejection on**.



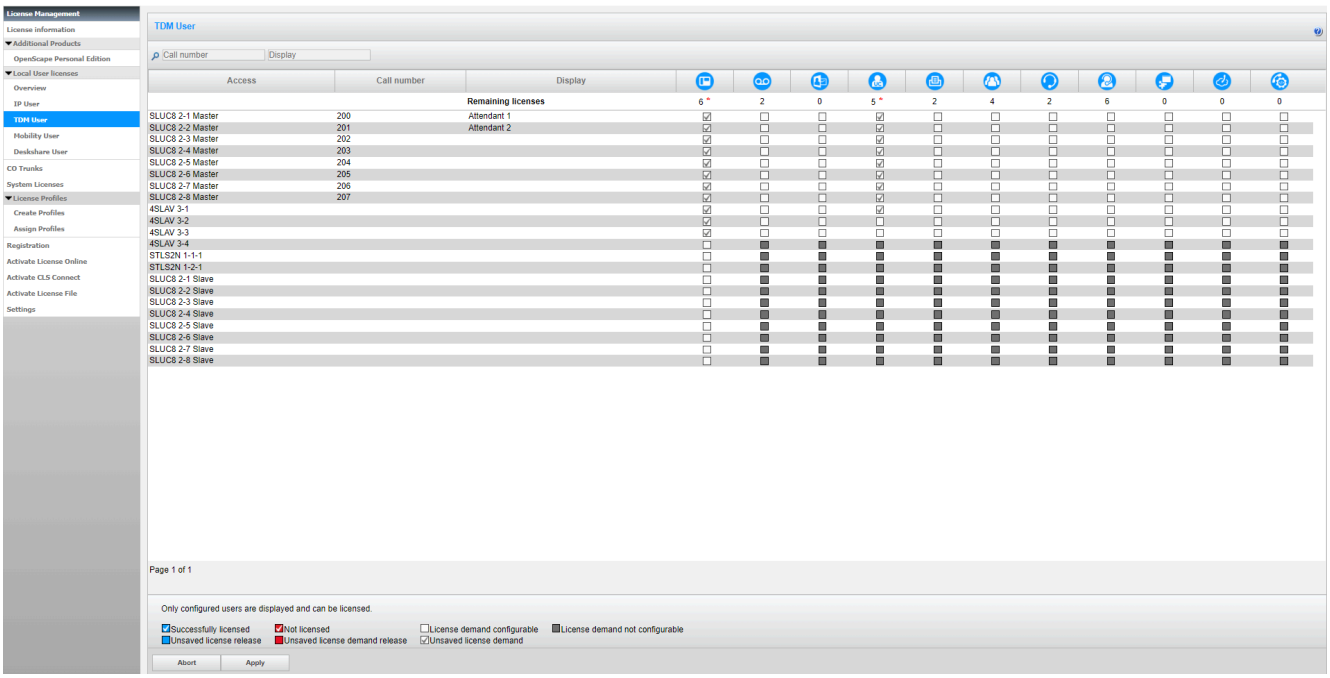
4) Configure the intercept criteria and Attendant codes (define the intercept options and call numbers for the Attendant Console).



5) Licensing the OpenScape Business Attendant



6) Licensing the presence status



7) Optional: when setting up an Attendant as an IP station, a password for the user account must be set up at the telephone.

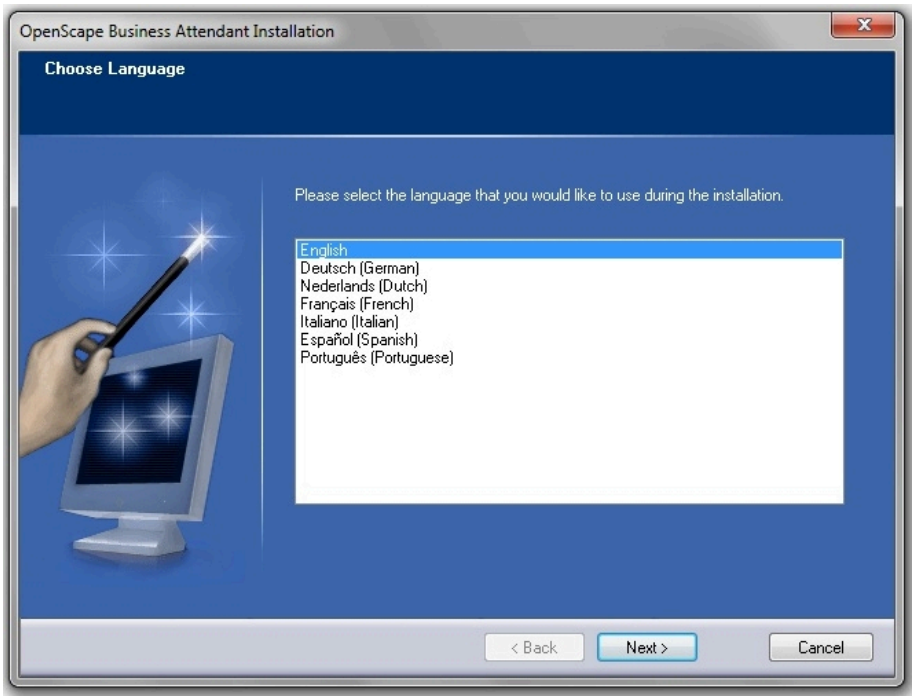


8) Install the USB driver

USB - COM driver (CallBridge) for optiPoint 500, OpenStage 30T and OpenStage 40T

USB - RNDIS driver for OpenStage 60T and OpenStage 80T

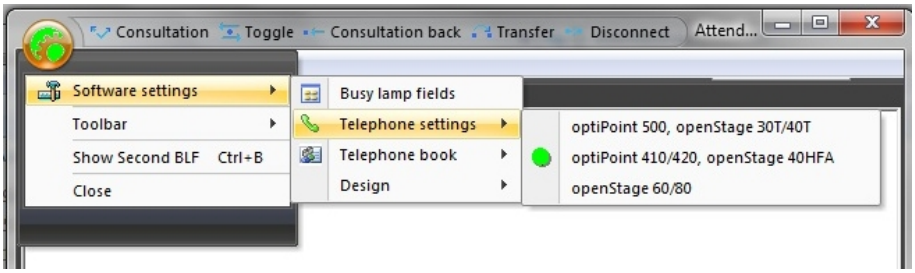
9) Install OpenScape Business Attendant via the installation routine (accept the license agreement, specify the storage location and the language of the OpenScape Business Attendant).

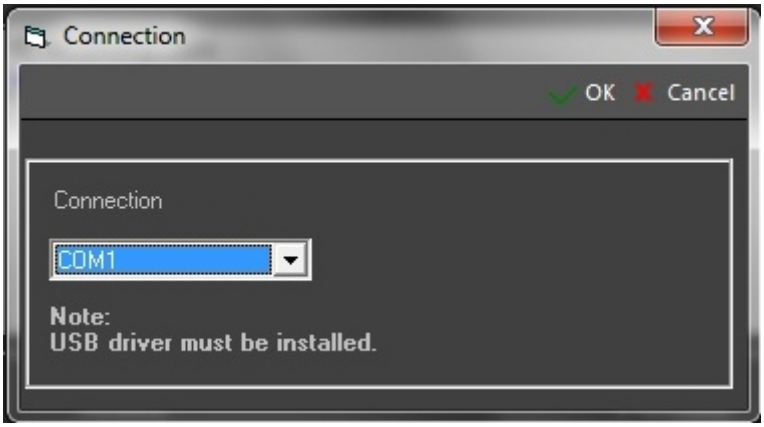


After the installation and the initial startup of the program, the configuration wizard starts automatically and requests the following settings:

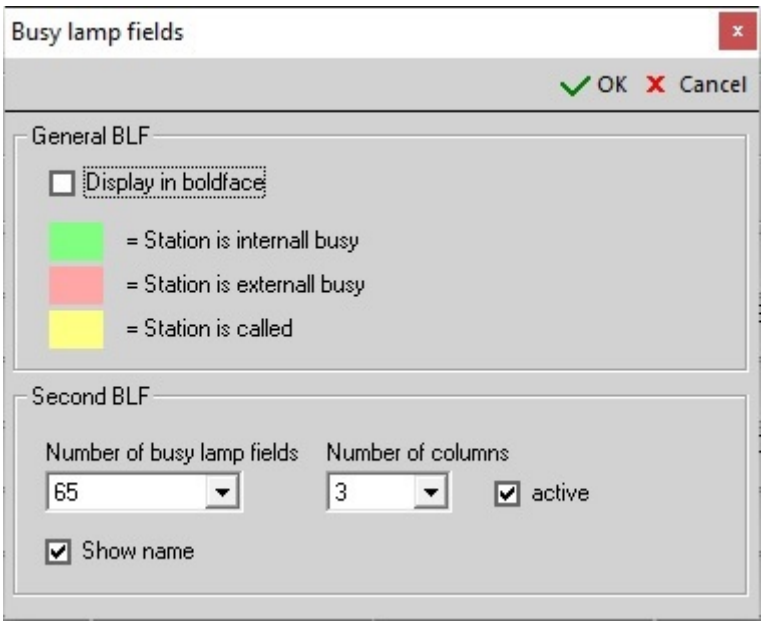
- Type of telephone
- Is the presence function to be used?

Configuration for access in the Attendant:

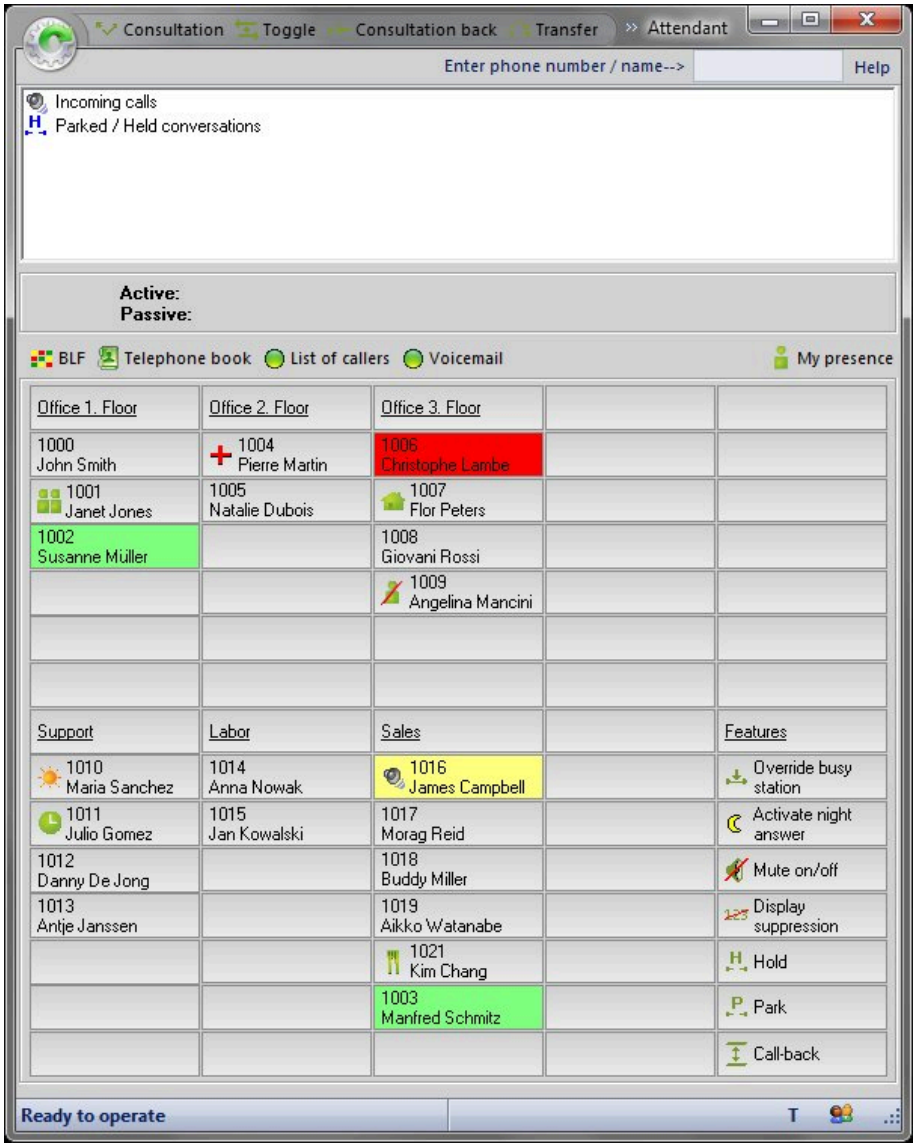




After logging into the communication system successfully, it is possible to fill the BLF automatically.



INFO: Assign or check the security settings (http or https) in the WBM.



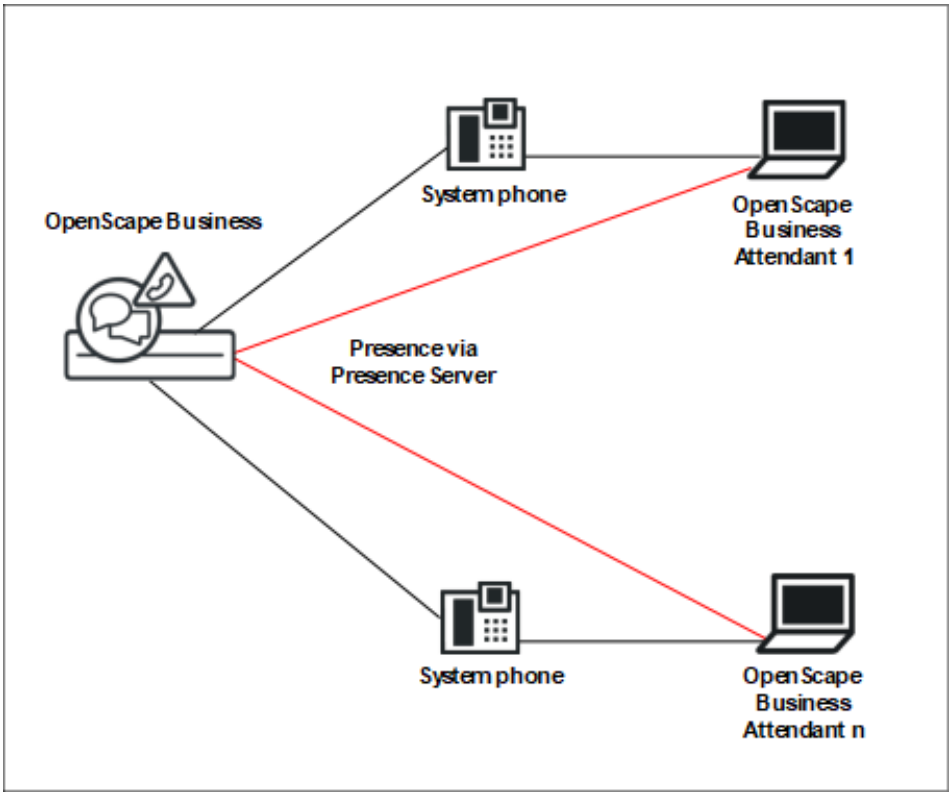
17.3.2.2 Scenario 2: Two or More OpenScape Business Attendants Connected to an OpenScape Business Single System

Prerequisites

The following prerequisites are required in addition to those for scenario 1:

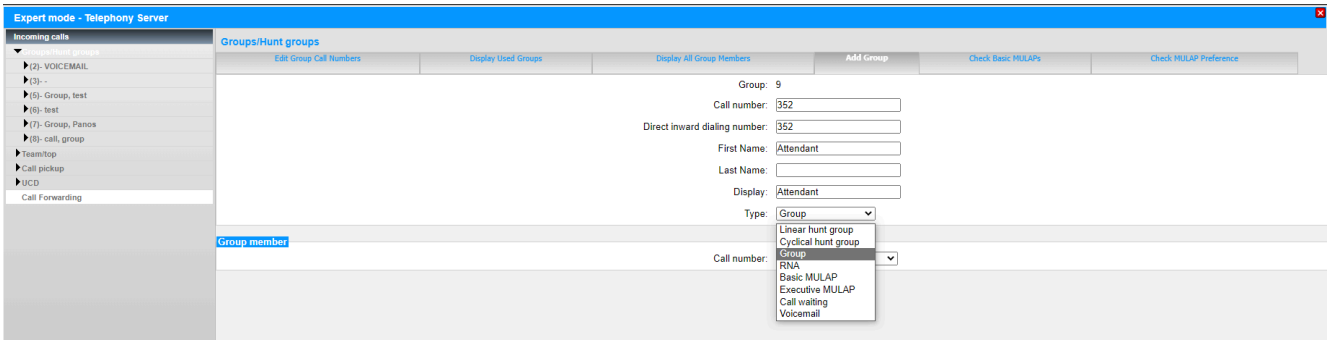
Sufficient licenses for UC Smart or UC Suite for presence information (optional)

Group configuration

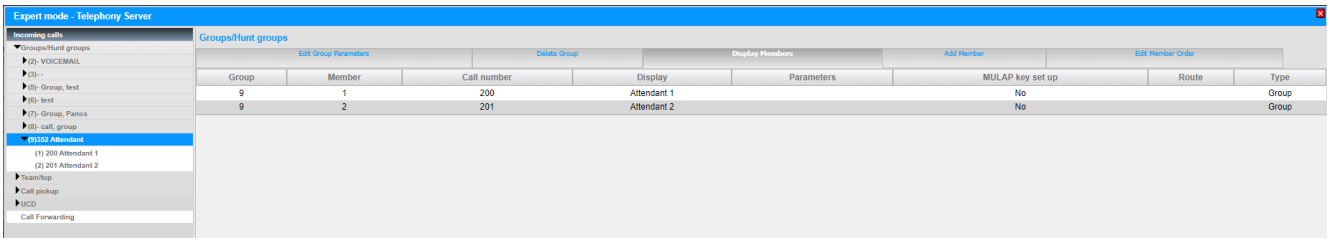


Step by Step

1) Set up as a station as an Attendant via the WBM (see Configuration Example 1).
2) Define a group; hunt groups (linear and cyclic) and call groups are supported.



3) Assign the attendants (the corresponding subscribers) to the group.



INFO: Configure the intercept criteria and Attendant codes (define the intercept options and call numbers for the Attendant Console). In these cases, the intercept position is the group phone number.

17.3.2.3 Scenario 3: OpenScape Business Network with Individual OpenScape Business Attendants (Network-wide BLF and Presence Status via WSI)

Prerequisites

License for UC Smart for presence information (optional)

Multiple OpenScape Business Attendants can be used in UC-Smart networks only. The WSI (Presence Server of OpenScape Business) provides netwide Hook states and Presence information. UC-Suite networks need myAttendant for netwide functionality.

17.3.2.4 Scenario 4: OpenScape Business Network with central OpenScape Business Attendant (Network-wide BLF and Presence Status via WSI)

Prerequisites

License for UC Smart for presence information (optional)

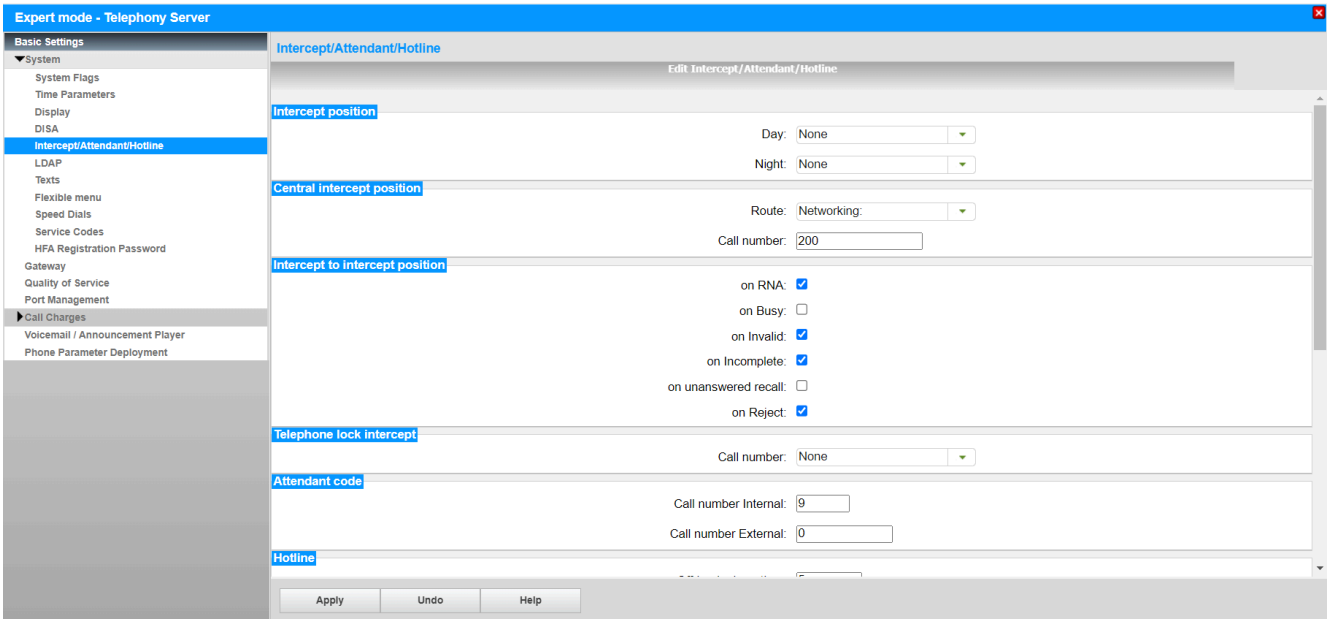
Multiple OpenScape Business Attendants can be used in UC-Smart networks only. The WSI (presence server of OpenScape Business) provides netwide Hook states and Presence information. UC-Suite networks need myAttendant for netwide functionality.

Central intercept position (in the node in which no OpenScape Business Attendant is set up)

Step by Step

1) Set up the OpenScape Business Attendant in accordance with configuration example 1.

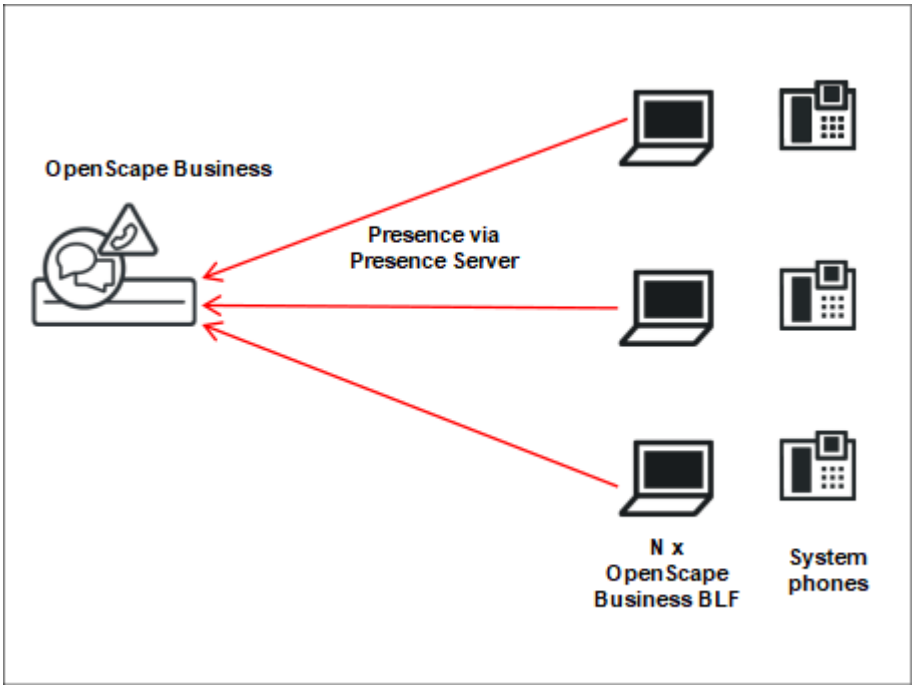
2) Enter the central intercept position in the node (where no OpenScape Business Attendant has been set up).



17.3.2.5 Scenario 5: OpenScape Business BLF Connected to an OpenScape Business Single System

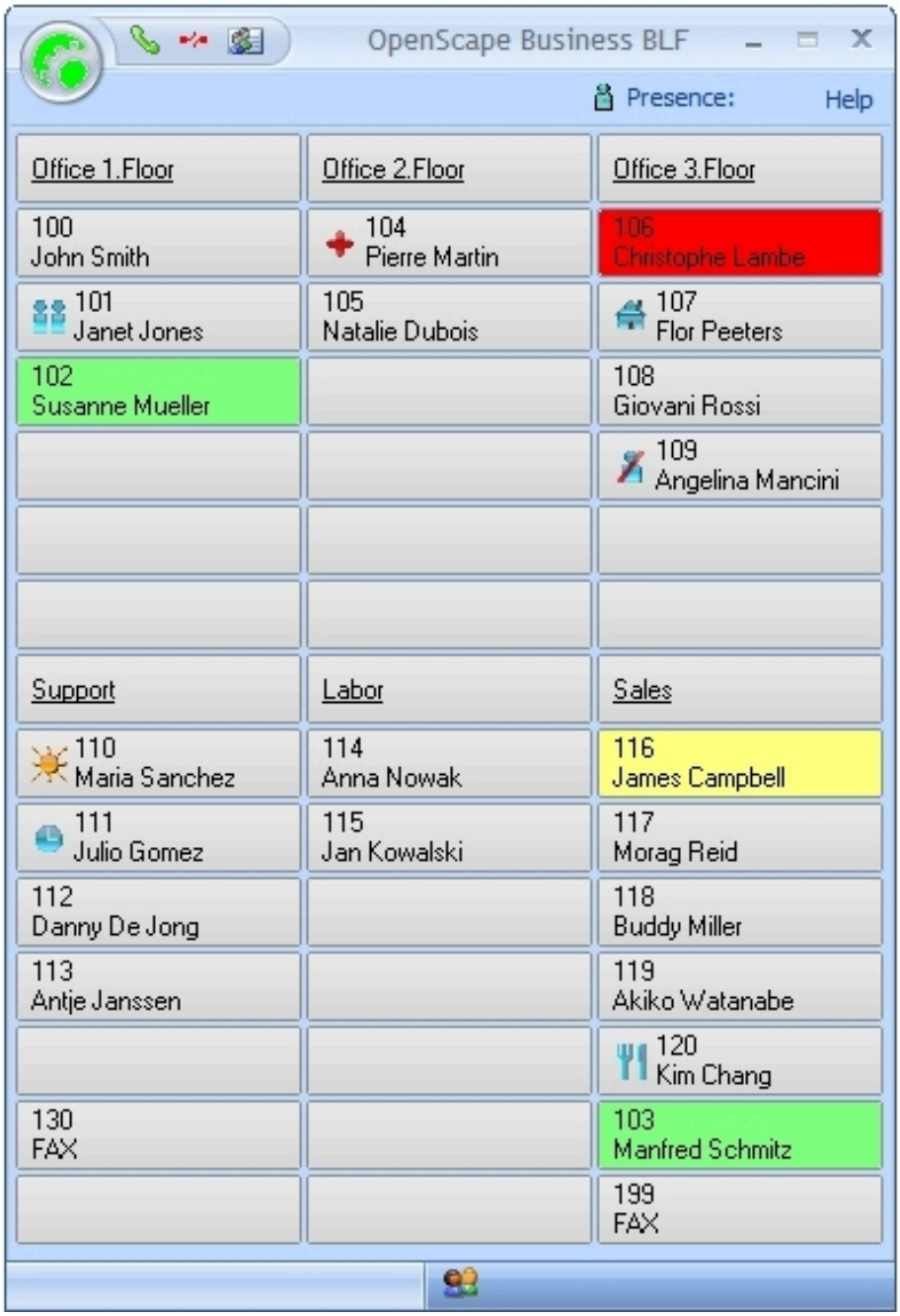
Prerequisites

- One OpenScape Business BLF license is available for each station
- The phones are already assigned
- One UC User license is available for each station



Step by Step

1) Configure the telephones via WBM
2) Configure the presence server via WBM
3) Install and start OpenScape Business BLF
4) The (optional) automatic assignment of the OpenScape Business BLF occur after the initial startup.



17.3.2.6 Scenario 6: OpenScape Business BLF Connected to an OpenScape Business Internetwork (BLF and Presence Status via WSI)

Prerequisites

- One OpenScape Business BLF license is available for each subscriber
- The phones are already assigned
- A UC User license is available for each subscriber
- OpenScape Business BLF can be used in UC-Smart networks, not in UC Suite networks. The WSI (Presence server of OpenScape Business) provides netwide Hook states and Presence information.

Step by Step

1) Configure the telephones via WBM

2) Install and start OpenScape Business BLF

3) The connection to the WSI and the manual assignment of the BLF occur after the initial startup. In this case, the BLF can be assigned for network-wide stations.

17.4 myAttendant

A wide range of Attendant functions are available to you via myAttendant. Subscribers can be easily managed here via user buttons. In addition, messaging functions (voicemail, faxes, instant messages, SMS, and e-mails) are available via the Message Center.

Main Attendant Functions

A maximum of 20 myAttendants can be connected per communication system (per node). The maximum configuration of the internetwork is equal to the total capacities of the networked communication systems. The presence and phone status are shown for all subscribers in the network. The Message Center of myAttendant shows the subscribers of the own communication system.

- Manage waiting or accepted calls
- The data of the active call is displayed
- Parked calls on hold are displayed
- Caller list
- Journal for open, scheduled, internal, external, answered, missed and outbound calls
- Directory (phonebook) application
  - LDAP (e.g., ODS)
  - Personal directory / Outlook contacts
  - Internal directory, for all interconnected stations in the network.

- Busy Lamp Field status of all internal subscribers of the own system as well as all stations of the network
  - Phone status: Free, Busy, Called, Forwarded, Do Not Disturb
  - Presence status (Office, CallMe, Meeting, Sick, Break, Out of the Office, Vacation, Lunch, Gone Home (netwide)

  NOTICE: The "sick" presence status may not be available, depending on system settings by the administrator.
- There are three interface styles to choose from.
- A maximum of 20 myAttendants can be connected per communication system (up to 20 licenses per OpenScape Business X3/X5/X8 and OpenScape Business S). The licensing of myAttendant occurs via the WBM.

Technical Requirements (see the Sales Information for Details)

- Standard Windows PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)
- Terminal server usage possible

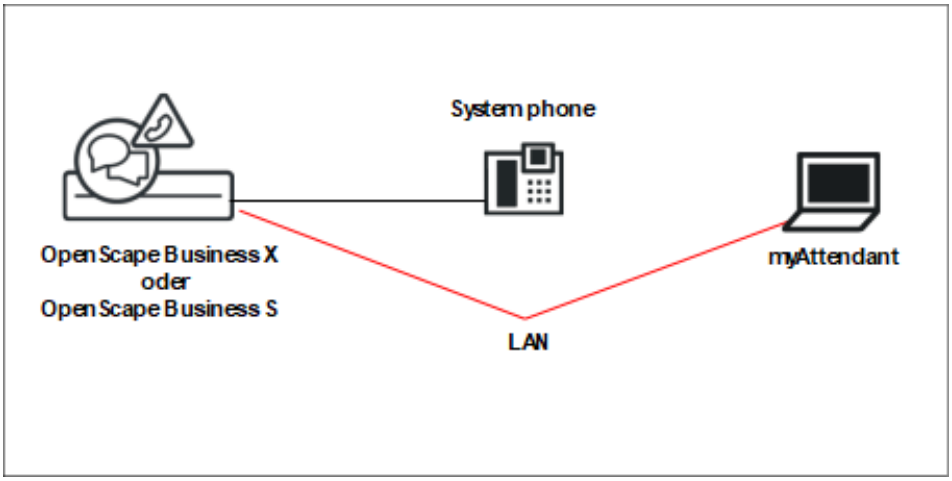
Additional Software

- Oracle Java 8 or higher or alternatively OpenJDK 8 (see **Service Center** > **Software**)

Supported Phones

- Openstage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/410/710 HFA
- SIP phones with RFC 3725 support, e.g., OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X SIP, OpenScape Desk Phone CP 110/210/410/710 SIP
- OpenStage 30T/40T/60T/80T

Simple plug and play installation; the first steps for the installation are sent to the user by the system (if his or her e-mail address has been configured).



17.4.1 Subscriber Management

Subscriber management is performed in myAttendant via user buttons, the internal directory, and the external directory.

User Buttons

The user buttons are located on the **Default** tab and are a part of the main window of 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.

The user buttons are sorted in alphabetical order by default.

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 Message Center

All voicemails, faxes, instant messages as well as SMS messages and e-mails are recorded and managed via the **Message Center** of myAttendant.

Messages can also be managed for other subscribers, provided these subscribers have granted the appropriate permission for this.

The Subscriber List window, contains a list of all communication system subscribers with their presence/absence status. Your own status is displayed first in a drop-down message overview. The other subscribers follow in alphabetical order.

Depending on what is selected in the message overview, message details are displayed, including a table of message-specific information that can be selected for further processing.

The various message types can be processed as follows:

- **Voice Messages (i.e., voicemails)** can be played back, deleted and forwarded,
- **LAN Messages** can be read, edited and deleted,
- **Fax messages** can be forwarded.

LAN Messages

LAN messages can be created only by myAttendant users. They serve as a kind of "bulletin board" for the subscriber, on which he or she enters notes (about individual subscribers). These messages can be viewed, edited or deleted, but cannot be sent to other subscribers.

17.4.3 Scenario 1: How to Configure a myAttendant connected to an OpenScape Business Single System

Prerequisites

The license for myAttendant is present.

Telephones with a valid license

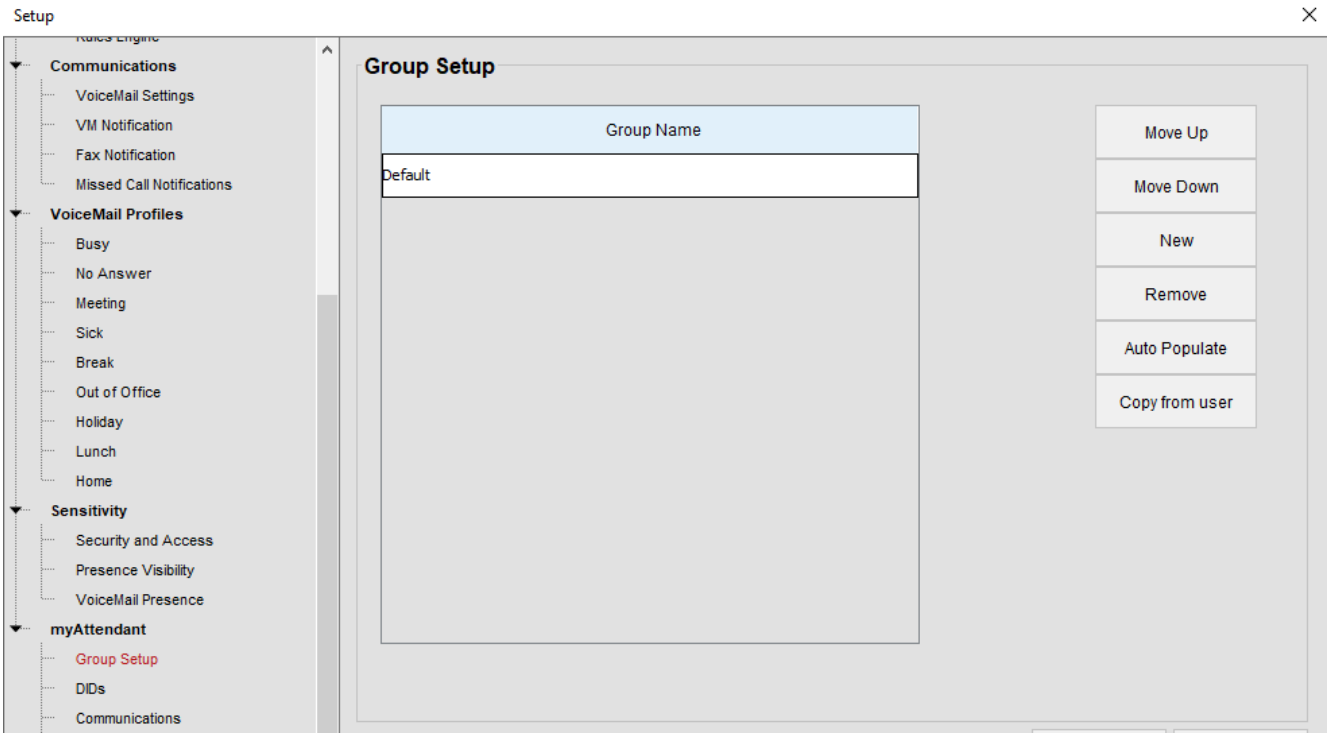
The Application Server or Application Board is available

UC Suite has been enabled via the Basic Installation wizard

Step by Step

1) Configure the Attendant Console using the WBM
2) Disable **Call waiting rejection** in **Expert mode**, under **Stations**>**IP Clients**>**System Clients**>**Stations**>**Edit Station Flags**.
3) Enable the feature **Immediately camp on for attendant calls** in **Expert Mode** under **Telephony Server**>**Basic Settings**>**System**>**Intercept**>**Attendant**>**Hotline**.
4) Check or change the intercept criteria and Attendant codes (define the intercept options and call numbers for the Attendant Console).
5) Licensing of myAttendant

6) After logging into the communication system successfully, it is possible to fill the BLF automatically. This can be configured in myAttendant under **Setup > myAttendant > Group Setup.**



17.4.4 Scenario 2: How to Configure Two or More myAttendants connected to an OpenScape Business Single System

Scenario 2 is based on scenario 1 and is configured additively.

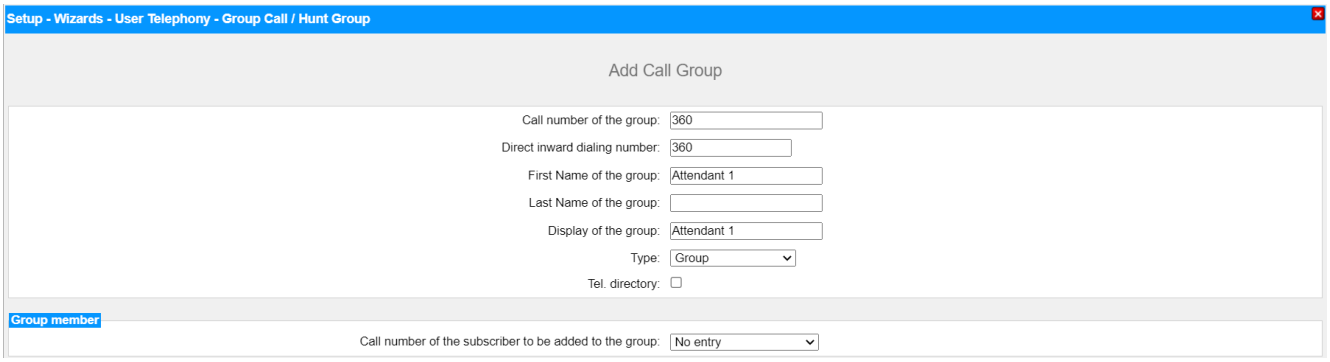
Prerequisites

Sufficient licenses for myAttendant

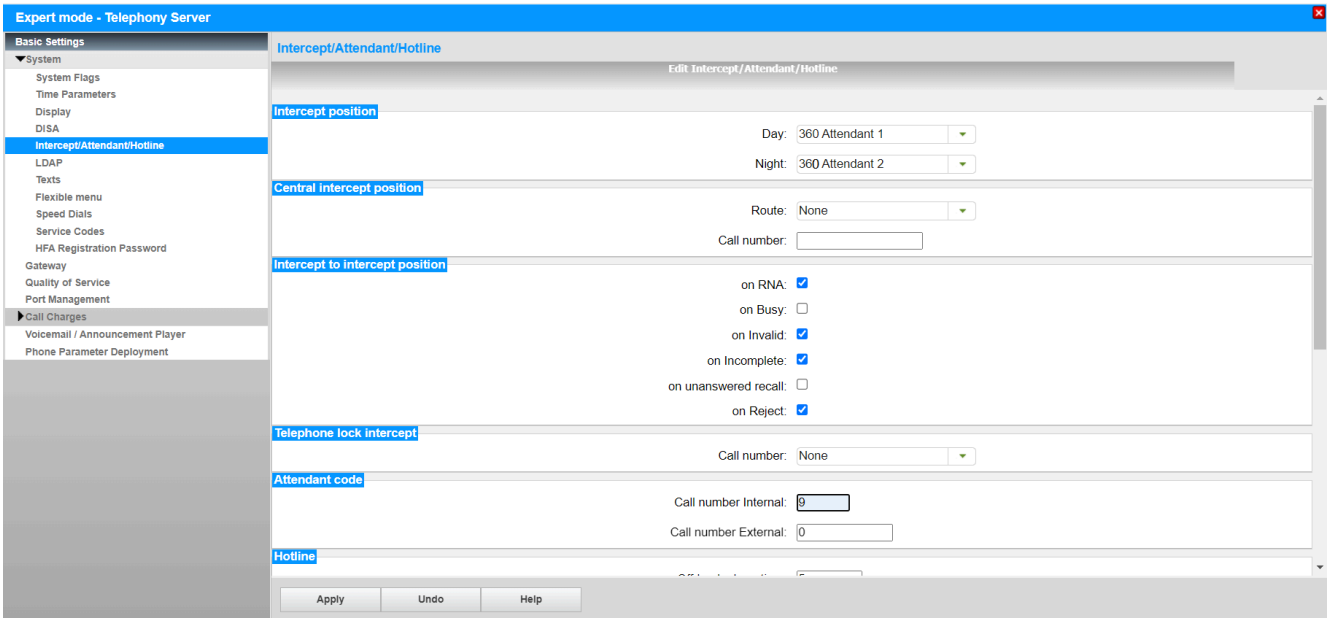
Telephone with a valid license

Step by Step

1) Configure a group (consisting only of Attendant Consoles) in the WBM under **Setup** > **User Telephony** > **Group Call / Hunt Group**>**Add**.



2) Select this group when configuring the OpenStage Attendant Console phones.



17.4.5 Scenario 3: How to Set Up an OpenScape Business Network with a Central myAttendant

Scenario 3 builds on scenarios 1 and 2 and is set up additively. Node 1 is linked to node 2. The central Attendant Console is in node 2.

Prerequisites

Sufficient licenses for myAttendant are available

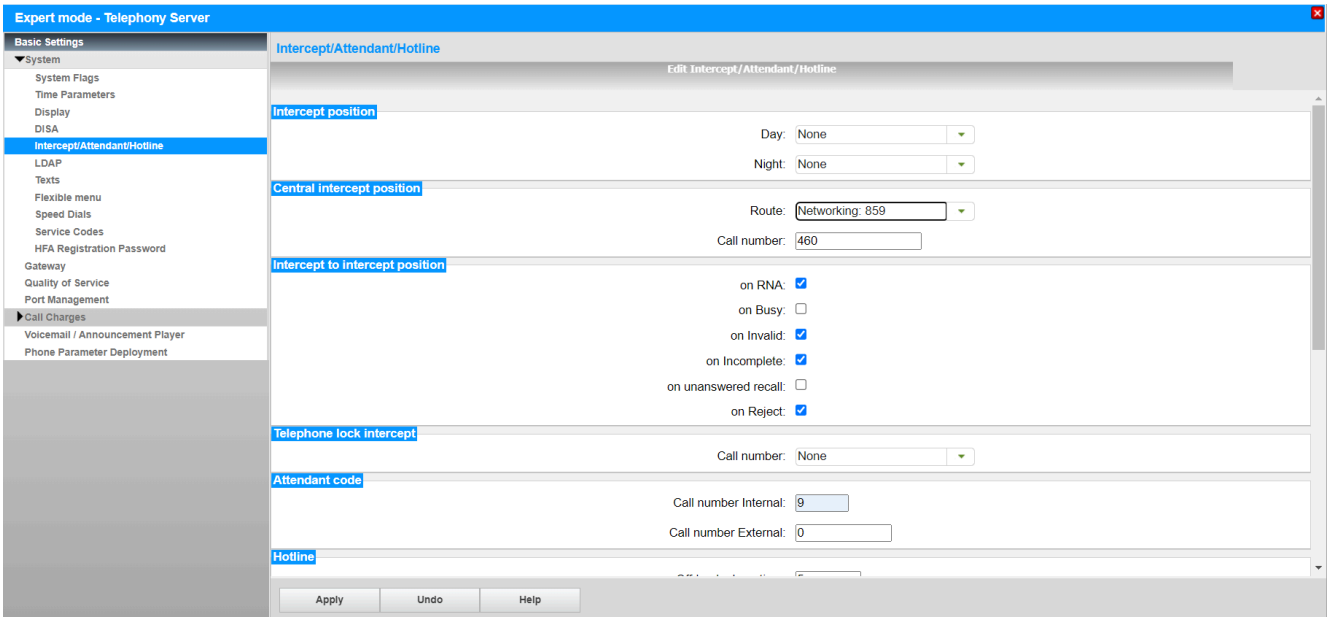
Licenses are available for networking

Telephone with a valid license

LCR is configured

Step by Step

1) Set up a central intercept position in node 1. The central intercept position must be created in a node in which NO Attendant Console is set up.



2) Set up the Attendant Console for system 2 (as described in Scenario 2).

3) Install myAttendant with the user data from node 2.

17.5 Intercept Position

The communication system diverts external calls that cannot be assigned to a station or answered to a set intercept position to ensure that no calls are lost. As an administrator, you can configure the intercept criteria.

The intercept position can be an individual station, a group or an announcement device:

- Intercept position (Attendant Console)
- Stations
- Hunt group
- MULAP group
- Group call
- External announcement device

A UCD group may not be selected as an intercept position.

If an intercept position is configured in the system, intercepted calls are forwarded to this intercept position. If no intercept position is configured, intercepted calls are signaled at the first IP station.

If an internal station is set up as an intercept position, the default key assignment is assigned to it automatically. In addition, the intercept position can be authorized for the Override feature.

As an administrator, you can assign one (two-digit) attendant code each to the intercept position for internal and external, under which the intercept position can be directly reached.

The intercept applies system-wide, i.e., identically for all subscribers in tenant systems. See also "Central Intercept Position in the Internetwork" in the section on Networking.

Intercept criteria

As an administrator, you can specify in which situations the Intercept feature is used via intercept criteria. The following intercept criteria are possible:

- On RNA (ring no answer)

  The call follows the entries in the call management (e.g., for a configured call forwarding). If no subscriber accepts the call, it is routed to the intercept position.
- On busy, if no additional forwarding is possible.

  The system first checks if call waiting is possible. If call waiting is not possible, the call follows the entries in Call Management (e.g., the call forwarding instruction configured). If no subscriber accepts the call, it is routed to the intercept position. Intercept on busy is only performed for first calls, not for forwarded or outgoing connections. A recall of an external station is not immediately intercepted when the destination station is busy; instead, call waiting is activated.
- On Invalid (misdialing)

  If the dialed station number is not configured or is inactive.
- On Incomplete

  If the Dialed station number is too short. Incomplete dialing is not evaluated if a central intercept position is used.
- On unanswered recall

  If an external call is not answered following an unscreened transfer (transfer before answer) and if the automatic recall to the original destination is also not answered, then an intercept is initiated after a preset time.
- On rejection

  If the call was rejected by an internal subscriber, the call follows the entries in the call management (e.g., for a configured call forwarding). If no subscriber accepts the call, it is routed to the intercept position.
- On missing phone number

  As for On Invalid.
- On chained call forwarding

  If a forwarded call encounters another forwarding instruction at the call forwarding destination, and the number of chained forwarding instructions allowed is exceeded, an intercept occurs. The number of chained forwarding instructions depends on the entries in the call forwarding. A maximum of 3 are allowed.
- On lock code

  If a subscriber at a telephone with an activated lock code dials a seizure code, an intercept occurs. A separate intercept is defined by the administrator for this purpose.
- On announcement (only with UC Suite)

  If a subscriber dials the (two-digit) attendant code while listening to a voicemail announcement or the AutoAttendant, an intercept occurs. A separate intercept is defined by the administrator for this purpose.

Dependencies

Topic	Dependency
Data calls	Data calls are disconnected, not intercepted.
Hunt group	Intercepts cannot extend beyond a hunt group; the call is forwarded to the first hunt group station and remains in the hunt group.
Default key assignment	The default key assignment has also the **View number of calls** key. This can be assigned to only 6 telephones. If the limit has been reached, no more default key assignments are made. The assigned default keys are not canceled when a device is no longer defined as an intercept position.
S_0 trunks	On S_0 lines, an evaluation takes place only when no day/night intercept position has been set up.
Night service	In order to reach the same destination from both the DID trunks and the MSI trunks while the Night service is active, the entry for Night Station number under Intercept > Attendant must be identical to the **Night Number** in **Ringing assignment per Line**.

17.5.1 How to Configure the Intercept Position and Intercept Criteria

The **Attendant Console** wizard can be used to configure the phone numbers for the Intercept position as well as the intercept criteria.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Attendant Console** wizard.
4) Enter the desired call numbers for the Intercept position in the **Attendant Console** and **Attendant code** (two-digit) areas.
5) Define the desired values in the **Intercept criteria** area.
6) Click on **OK & Next** followed by **Finish**.

17.5.2 How to Configure the Central Intercept Position

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.

3) Click **Basic Settings** > **System** > **Intercept/Attendant/Hotline** in the menu tree.
4) Select the desired entry from the **Route** drop-down list in the **Central intercept position** area.
5) Enter the desired **Call number** in the **Central intercept position** area for **Day** and **Night**.
6) Click on **Apply** followed by **OK**.

17.5.3 How to Configure the Telephone Lock Intercept

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **Basic Settings** > **System** > **Intercept/Attendant/Hotline** in the menu tree.
4) Select the desired item in the **Telephone lock intercept** area from the **Station Number** field.
5) Click on **Apply** followed by **OK**.

17.5.4 How to Configure the Intercept Announcement

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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 Multimedia Contact Center

The Contact Center is a powerful solution for the optimal distribution and handling of incoming calls, faxes and e-mails. Intelligent, skills-based routing ensures that callers are always connected to the most qualified agent, regardless of the contact medium. A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. myReports provides a number of report templates for analyzing the Contact Center operations.

The Multimedia Contact Center is fully integrated in the UC Suite software. It includes all required software components. The Contact Center functions themselves are released through licenses.

The Contact Center uses the resources of the communication system such as queues for incoming calls and unified communications functions to record and play back announcements.

The central software component of the Contact Center controls all routing functions for incoming calls, faxes, and e-mails and also controls the LAN-connected PC workplaces of agents and wallboard displays.

On the PC workplaces of agents, the myAgent application is installed. The myReports application can be optionally installed to generate and send reports. The required software can be downloaded directly from the download area of the communication system and installed on the client PC.

The WBM is used to set up the Contact Center basic functions, schedules, distribution rules as well as the agents. The settings for the daily operation of the Contact Center such as the assignment of agents to queues, for example, can also be made directly via myAgent.

If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), a fallback solution can be implemented via the UCD feature of the communication system. Distribution rules for emergencies must be taken into account when setting up UCD groups within the framework of the initial setup of the Contact Center.

INFO: Information on the UC Suite and the unified communications features can be found in the UC Suite chapter.

18.1 Contact Center Clients

A number of convenient functions for handling and wrapping up calls, faxes and e-mails are offered to the Contact Center agents via the myAgent application. The myReports application can be used to generate reports on the calls, queues, agents, performance, GOS (Grade of Service) and wrapup codes of the Contact Center. More than 100 predefined report templates are available.

18.1.1 myAgent

Convenient functions for handling and wrapping up calls, faxes and e-mails are available to all agents via myAgent.

myAgent provides the following features:

- Processing of
  - Make Call
  - Faxes
  - E-mails
- Callback function for agents
- Displaying and changing the agent status
- Displaying and changing the presence status of internal subscribers of the communication system
- Real-time presentation of queues
- Recording of calls, if activated in the communication system
- Instant messaging
- Request for assistance through
  - Supervision of calls (depending on country)
  - Overriding calls
  - Instant Messaging
- Integration of the internal directory, external directory, external offline directory (LDAP) and Outlook Contacts for searches by name
- Creation of reports based on predefined report templates

Depending on the authorization level assigned to an agent, either a set of standard functions (agent) or advanced functions (Supervisor or Administrator) are available to the agents in myAgent (see Agent Functions Independent of the Authorization Level).

The assignment of agents to queues occurs using the myAgent application. Only an agent with the authorization level of a Supervisor or an Administrator can make this assignment. The following properties, which affect the distribution of calls, faxes and e-mails in a queue, can be assigned here to the agents (agent assignment (binding)):

- **Primary Agent** or **Overflow Agent**

  Calls are distributed uniformly to primary agents. An overflow agent receives a call only when the number of calls exceeds a defined number ow when a call has exceeded a specified waiting period.
- **Enable agent callback**

  Agent callback enables a caller in the queue to leave a voicemail for agents. As soon as an appropriate agent becomes free, that agent receives a call, hears the voicemail left by the caller, and can then call back that caller.
- **Skill Level**

  Skill levels control the distribution of calls to agents in call queues. Agents with higher skill levels are given precedence when calls are distributed. In cases where all agents have the same skill level the longest idle agent receives the call.
- **Work time**

  The work time enables agents to finish any tasks, e.g., administrative tasks, that may be required after completing a call and before receiving the next call.
- **Overflow after calls in queue**

  Calls that exceed the maximum number are received by an overflow agent.

- **Overflow after seconds in queue**

  Calls that exceed this waiting period and received by an overflow agent.

The **agent binding list** area shows agents with the authorization level of a Supervisor or Administrator which agents are assigned to which queues. Agents with the agent authorization level can only see the queues to which they are assigned.

18.1.2 Prerequisites for myAgent

In order to use myAgent, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

INFO: Please make sure that you refer to the current notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Telephones

myAgent can be used in combination with the following telephones:

- 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)

Older devices (such as optiPoint 410/420/500 and Gigaset M2/SL3/S4/SL4/S5) are supported. Optiset E devices cannot be operated. myAgent cannot be used with SIP stations, Mobility stations, virtual stations, groups or MULAP stations. Details on the tested and released telephones can be found in the Release Notice.

Operating Systems

myAgent can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for myReports for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Additional Software

- Oracle Java 8 or higher or alternatively OpenJDK 8 (see **Service Center** > **Software**)
- Adobe Reader 9 or later (for reports in PDF format)

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

Microsoft Terminal Server, Citrix XenApp Server

myAgent can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

INFO: Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

INFO: Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) with Citrix XenApp 6.5 Server (Desktop Mode)

Support for myAgent for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Service Center** and makes them available to users via a network drive, for example.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

INFO: The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

18.1.3 myReports

Agents with the Supervisor or Administrator authorization level can use myReports to generate reports about agents and their activities, calls, queues, performance, GOS (Grade of Service) and wrap-up codes.

myReports offers the following features:

- More than 100 predefined report templates sorted by subject area (report groups) for the creation of reports
- Schedules for the scheduled generation of reports
- Immediate or scheduled sending of reports by e-mail
- Scheduled export of reports
- Output formats for report previews, sent e-mails and exported reports: Excel, PDF, and Word
- Report preview to check a report to be created in the desired output format.

User Roles

myReports has its own user management, which controls access to the functions of myReports through user roles. A distinction is made here between the myReports users (standard user) and the myReports administrator.

The current user role is set when you log into myReports.

The differences between the roles are summarized in the following table.

myReports: Activity	User Role	
	myReports User	myReports Administrator
Reports		
Preview report	X	X
Send report immediately by e-mail	X	X
Add report template	X	X
Delete added report template	X	X
Define new report template		X
Update predefined report templates		X
Schedules		
Add a schedule	X	X
Display details of a schedule	X	X
Edit schedule	X	X
Delete schedule	X	X
Configuration		

myReports: Activity	User Role	
	myReports User	myReports Administrator
Change language of user interface	X	X
Change color of user interface	X	X
Configure e-mail template	X[7]	X
Change server address	X	X
Change administrator password		X
Configure prefixes for external phone numbers		X
Enable/disable data protection		X
Configure the storage location for the export of scheduled reports		X
language, selecting		X[8]
Set up default language		X[8]

18.1.3.1 How to Reset the myReports Administrator Password

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server**.
4) Click on **Maintenance**.
5) Click on **Reset Password**, under the **Reports** area.

Next steps

Inform the myReports administrator(s) that you have reset the administrator password to the default password `reports`.

18.1.4 Prerequisites for myReports

In order to use myReports, the client PC of the subscriber must be equipped with the appropriate hardware and software configurations.

[7] The administrator password must be entered to configure the e-mail template

[8] In order to configure languages and set the default language, you will need to log in as a myReports administrator with a special password.

INFO: Please make sure that you refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

Operating Systems

myReports can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Support for myReports for Microsoft Windows XP and Microsoft Windows Server 2003 will end at the same time as the end of support for these products by Microsoft. The product will still be supported, but will no longer be tested in detail.

Additional Software

- Oracle Java 8 or higher or alternatively OpenJDK 8 (see **Service Center** > **Software**)
- Adobe Reader 9 or later (for reports in PDF format)
- Microsoft Excel 16 / 2013 / 2010 (for reports in Excel format)
- Microsoft Word 16 / 2013 / 2010 (for reports in Word format)

Minimum Hardware Requirements

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbps LAN (1 Gbps LAN recommended)
- XGA (1024x768) screen resolution, myPortal for Outlook: SVGA (800x600) screen resolution

Multi-user PCs

Under Microsoft Windows 7 and Microsoft Windows Vista with multi-user PCs, every local user can use myReports with his or her own custom settings, provided the first local user has installed the client with local administration rights. Only the first local user with local administration rights can perform updates via the AutoUpdate.

Microsoft Terminal Server, Citrix XenApp Server

myReports can be used in Microsoft Terminal Server and Citrix Server environments under the following preconditions:

INFO: Terminal Server and Citrix Server environments, including hosted services and virtual environments are the responsibility of the customer.

INFO: Citrix server environments can decode some regional characters (e.g., German umlauts) correctly.

Operating systems:

- Microsoft Windows Server 2015 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 bit / 64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) as Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 bit) with Citrix XenApp 6.5 Server (Desktop Mode)

Hardware Prerequisites: The number of installable clients depends on the server performance and on the amount of available memory. If the server is also being used for other applications, their memory requirements must also be taken into account.

More information on the configuration of Citrix XenApp Server can be found under:

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

Installation Files

The following options are available for providing installation files to users:

- The administrator downloads the installation files from the **Service Center** and makes them available to users via a network drive, for example.

Please refer to the notes in the `ReadMe first` file, which is located in the storage directory of the install files.

INFO: The automatic distribution of the MSI file via a deployment service with Microsoft Windows Server is not supported.

18.1.5 Notes on Using myAgent and UC Suite Clients Simultaneously

When myAgent and other UC Suite clients are used simultaneously via one UC Suite user account, the possibility of mutual interactions cannot be excluded.

The term myPortal is used generically in this section to represent myPortal for Desktop, myPortal for Outlook, myPortal @work and myPortal to go.

Examples of mutual interactions:

- Changing the presence status via myPortal

  The examples apply to the default **Voicemail** setting for all call forwarding destinations.

  – myAgent: Agent is logged on.

    myPortal: The automatic reset of the presence status to Office is disabled.

    Changing the presence status via myPortal causes the agent to be immediately logged out of the queue(s). After the agent logs off via myAgent, the presence status in myPortal is reset to **Office**.

    A change in the agent status via myAgent (e.g., to **Break**) is registered by myPortal, but this does not apply to **Log in**, **Log out** and **Work Time**.

  – myAgent: Agent is logged on.

    myPortal: The automatic reset of the presence status to Office is enabled.

    If the agent changes his or her status via myAgent to **Break**, he or she will be automatically available again after the break time has expired.

    A change of the presence status via myPortal to **Break** causes the agent to be immediately logged out of the queue(s).

  – myAgent: Agent is logged on.

    A change of the presence status via myPortal to **Do Not Disturb** causes the agent to be immediately logged out of the queue(s).

- Outbound Calls via myPortal

  The presence status of the subscriber is visible via myAgent.

  The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.

- Incoming calls to the station number of the agent

  The presence status of the subscriber is visible via myAgent.

  The calls appear only in the journal of myPortal. No transfer to the statistics of the Contact Center occurs, since these are not Contact Center calls.

- Recording a call

  The recording of calls via myPortal is not registered by myAgent. myAgent offers this function even if the recording of a call is already occurring via myPortal.

18.2 Agents

The agents (stations) of a queue comprise a workgroup and are typically deployed for technical hotlines, for example, or in order processing, order acceptance, CRM, etc. The incoming calls, faxes and e-mails are distributed uniformly to the available agents for a queue.

In order to use a station of the communication system as an agent, this station must first be configured accordingly. The rights of the individual agents are defined by selecting their respective authorization levels (Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges (see Agent Functions Independent of the Authorization Level).

An agent can be defined as a permanently available agent. Such agents remain available for calls, faxes and e-mails even when they do not accept a call, fax or e-mail.

18.2.1 Agent Functions Independent of the Authorization Level

When a user is configured as an agent, the rights of the agent are defined by selecting the appropriate class of service for that agent (i.e., the authorization level as an Agent, Supervisor or Administrator). An agent with the authorization level of a Supervisor or Administrator has elevated privileges.

The differences between the authorization levels are summarized in the following table.

myAgent:	**Authorization level (class of service)**		
Activity	**Agent**	**Supervisor**	**Administrator**
Assign an agent to a queue	–	X	X
Move an agent to another queue	–	X	X
Remove an agent from the queue	–	X	X
Change the status of an agent	–	X	X
Display / hide the agent binding list	Assigned queues	All queues	All queues
Edit an agent assignment	–	X	X
Display list of Live calls	Assigned queues	All queues	All queues
Activate myAgent screen pop automatically for alarms	–	X	X
Activate alarm tone	–	X	X
Display wallboard	Assigned queues	All queues	All queues
Display the Grade of Service graph	Assigned queues	All queues	All queues
Display the Average Times graph	Assigned queues	All queues	All queues
Move call to first position in a queue	–	X	X
Record a call	Current call	All calls	All calls
Save recording of call as WAV file or send as WAV file by e-mail	–	X	X
Save fax as a TIFF file or send by e-mail	–	X	X
Save e-mail as EML file or send as EML file by e-mail.	–	X	X
Call supervision (country dependent)	–	X	X
Override a Call	–	X	X
Accept a request for assistance	–	X	X
Create reports	–	X	X
Open WBM	–	X	X

18.2.2 Preferred Agents

Every caller (e.g., every calling customer) can be assigned one or more preferred agents of a queue. In such cases, the communication system first tries to switch the caller and his callback requests through to a preferred agent. If multiple preferred agents have been specified, a priority (sequence) can be defined to determine the order in which these agents are connected.

If no preferred agent is available, the call is forwarded to any available agent.

18.2.3 Agents in multiple queues

An agent can be assigned to multiple queues with different skill levels. In such cases, the function of the agent as a primary agent or an overflow agent must be defined.

18.2.4 Contact Center Breaks

In order to allow every agent the chance to take a defined break, Contact Center breaks of different lengths can be defined (e.g., for lunch or a cigarette break). Contact Center breaks are available system-wide and can be selected by an agent via myAgent as required.

18.2.5 Agent Login/Logout via Telephone

Login/Logout into the Contact Center is supported also via phone without the need to run myAgent in order to use the Contact Center functions. If an agent has been logged in via phone only voice calls can be processed. PopUp Window and WrapUp Code entry are not supported in this case. This applies also if myAgent is active and agent logs into the Contact Center using the phone. Full functionality of myAgent can be regained if the agent logs out via the phone and then logs in via myAgent.

Prerequisites and Constrains

- OpenScape Business Contact Center functions via telephone only work for agents for which a myAgent license is assigned within OpenScape Business
- All functions are only supported on such phones, which are released for use with OpenScape Business Contact Center
- In case that login via phone is successful and the associated myAgent client is not active, only Voice Calls are routed to the agent
- In case that login via phone is successful and the associated myAgent client is active, Email / Fax and Callback Calls are not be presented to agent if he logs in via phone. In this case screen-pops and wrap up work as usual but only voice calls will be delivered to the agent. To get full functionality, agent has first to logout via phone mode and login afterwards via myAgen

Login to Contact Center via Telephone

When the agents log into OpenScape Business Contact Center via the telephone, independent from myAgent client and Contact Center is active:

- The UCD functions for login are used at the phone
- The login function can either be executed via feature code or by a programmed key
- Agent is logged into all queues, to which he is assigned within the Contact Center configuration
- Telephone display informs agent about the login status
- Only UCD queue information (e.g. calls in queue information) is displayed on demand

The agent can use the following functions:

- Logon / Logoff (with UCD Agent ID)
- Wrap Up
- Available/Unavailable
- Display of calls within UCD Queue to which the UCD Agents ID has been assigned

NOTICE: UCD Night Service must not be used by the agent.

NOTICE: myAgent permanent available flag is supported for login via Phone. This means that in case an agent is logged in with his/her phone and a call was missed, this agent stays available for the next call. This is the same behavior as with using myAgent client.

In case that Contact Center fails during agent is logged on, the agent stays logged on into UCD and voice calls are routed as configured within the UCD routing. In case that agent was not logged in he can log into UCD via telephone.

Logout of Contact Center via Telephone

When the agents log out of OpenScape Business Contact Center via the telephone, independent from myAgent client and Contact Center is active:

- The UCD functions for logout are used at the phone
- The logiout function can either be executed via feature code or by a programmed key
- Agent is logged out of all queues, to which he is assigned within the Contact Center configuration
- Telephone display informs agent about the logout status
- No other Contact Center / UCD information (e.g. calls in queue information) is displayed

Set agent available/unavailable via Telephone

When an agent sets his status to available / unavailable for contacts routing of OpenScape Business Contact Center via telephone independent from myAgent client and Contact Center is active:

- Telephone display informs agent about the login status
- In case that myAgent is not active only voice calls shall be routed to the agent

Set/Reset Working after call (Wrap Up) via Telephone

When an agent sets his status to "Working after call" (Wrap Up) via telephone independent from myAgent client and Contact Center is active, it does not route any calls to the agent until the agent's specific Wrap up time, which is configured within OpenScape Business Contact Center, is expired or agent has reset Wrap Up via telephone.

Status Mapping

Agent status change via phone is mapped as follows to myAgent agent status:

Phone Device			myAgent			
Feature Code	**Feature Code**	**Description**	**Phone Display Text**	**Status**	**Additional Text**	**Remark**
*401	UCD Agent ID	Log on UCD agents	Available	Available	-	Agent is set as available in all assigned queues
#401	–	UCD - agent log off	Not Available	Not available	-	Agent is set as not available from all assigned queues
*402	–	UCD - agent available	Available	-	-	Available (end of Work Time)
#402	–	UCD - agent not available	Not Available	Work Time	countdown from 999.999 seconds	-
*403	–	UCD work on	Wrap up	Work Time	countdown of configured worktime	Work time must be finished before it can started again. No work time cumulating like in myAgent. After work time is elapsed agent is set available automatically.
#403	–	UCD work off	Available	Available	-	-
*404	night service target	UCD night service on	–	Not supported	-	UCD Night Service must not be used
#404	–	UCD night service off	–	Not supported	-	UCD Night Service must not be used

Phone Device				myAgent		
Feature Code	**Feature Code**	**Description**	**Phone Display Text**	**Status**	**Additional Text**	**Remark**
*405	–	UCD - calls in queue	-	-	-	Only the queue to which the UCD agent ID has been assigned is shown, regardless if the agent is assigned to multiple queues within the Contact Center

18.3 Queues and Schedules

Queues are the basis of the Contact Center. Calls, faxes and e-mails for a queue can be handled, depending on the skill levels of agents, the priorities and waiting periods. Announcements can be played for waiting callers. A schedule is used to define how incoming calls are to be handled on certain days and at specific times.

18.3.1 Queues

As a rule, call distribution occurs by sending any incoming call, fax or e-mail for a queue to the specific station in the group (i.e., the agent) whose last call lies furthest in the past. It is also possible to define other distribution rules (based on the different skill levels of agents, for example). If all agents are busy, any additional calls, faxes and e-mails are placed in the queue and then distributed to the next free agent based on their priority and the waiting time.

Schedules and the rules contained in them (i.e., the CCVs or call control vectors) can be used to define how a call to a queue at a specific time and on a specific date is to be handled. The rules define which announcement is to be played back to callers, for example, or where a call is to be forwarded.

Faxes, e-mails and agent callbacks are assigned to queues directly, independently of schedules.

When assigning agents to queues, different properties, which affect the distribution of calls in a queue, can be assigned to agents (e.g., Primary Agent or Overflow Agent and Skill Level). Agents can be assigned to queues

- via the WBM by an administrator with the **Advanced** profile.
- via the application myAgent by an agent with the Supervisor or Administrator authorization level.

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.

The following main settings can be made for queues via the WBM:

- Activating, deactivating and deleting queues

  Note: After the deletion of a queue, no reports for past time periods can be generated. Queues that are no longer required should be deactivated.
- Configuring queue alarms

  You have the following options:

  – Queue Alarm Count (alarm threshold value): If the number of calls waiting in the queue exceeds the number specified here, the queue symbol for the agent changes from green to orange. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
  – Queue Alarm Time (alarm threshold value): If the waiting time for a queued call exceeds the time specified here, the corresponding item in the list of Contact Center calls for the agents changes to red. Agents with the Supervisor or Administrator authorization level can set whether they should be warned with an alarm tone and whether myAgent should be automatically brought to the foreground with a screen pop.
- Defining timeouts for missed calls, faxes and e-mails

  If a phone call, fax or e-mail is not accepted by the agent at the end of the time specified here, the call, fax or e-mail will be forwarded to the next available agent.
- Defining an abandoned call threshold

  The time specified here determines whether or not an abandoned call is included in the statistics (i.e., in a report). Calls abandoned after the specified time has elapsed are included in the statistics.
- Configuring queue depth

  Control of the maximum number of active and waiting calls in a specific queue. The Contact Center indicates to the system that the defined threshold of the queue size is reached. As a result the system rejects every new incoming call for the appropriate queue before the call is connected with the system, until the number of calls falls below the threshold.

  The maximum queue size is determined by following parameters:

  – Maximum number of waiting positions within the queue. (WLS = Waiting Loop Size)
  – Maximum number of active and waiting calls of the queue.(Queue Depth Size).
- Setting up inbound fax pilots

  If configured, station numbers can be selected for incoming Fax messages. Faxes to these phone numbers will then be added to the queue and treated as incoming calls.
- Setting up an inbound e-mail service

  Multiple e-mail addresses can be set up for a queue. E-mails sent to these addresses are placed in the queue and treated like incoming calls.
- Setting up a return e-mail address

  E-mail address of the queue, which is displayed to the recipient when an e-mail is sent by an agent.

- Activating intelligent call routing

  An incoming call is forwarded to the agent with whom the caller was last connected, provided no preferred agent was defined for that caller.

18.3.2 Schedules

For each queue, a schedule can be defined with rules (Call Control Vectors or CCVs) to determine how incoming calls are to be handled on specific dates and at specific times.

For example, on work days, separate rules may be defined for the morning shift (from 6:00 to 14:00 hours), the afternoon shift (14:00 to 22:00 hours) and the night shift (from 22:00 to 06:00 hours). Similarly, a weekend rule can defined for the weekends. For each of these rules, you can define whether an announcement is to be played, for example, and/or the destination to which the calls are to be forwarded.

Schedules are the core of the Contact Center configuration. Without the definition of at least one schedule, the configuration of a Contact Center cannot be completed successfully. Every queue must be assigned at least one schedule. This may also be the same schedule in every case.

A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls for a queue are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects and can be saved under a user-defined name upon completion.

Saved rules can be assigned to one or more schedules as a default rule (default CCV) or an exception rule (exception CCV). They can be opened, edited and saved again at any time by using the rule editor.

After a schedule has been assigned a default rule (default CCV), this schedule can be saved under a user-defined name. A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules of a queue.

Rule Editor (CCV Editor)

The Rule Editor is used to create rules from predefined CCV objects. The arrangement of the CCV objects and their properties determine how incoming calls are to be handled.

NOTICE: A rule has an upper limit of 500 CCV objects.

The following predefined CCV objects are available:

INFO: For all of the named CCV objects, the two general properties listed below also apply:

Description: Optional entry to describe the CCV object, e.g., Greeting.

Process digit: specification of the digit(s) required without blanks, commas or other characters. The specification refers to the preceding CCV object. If 9 was specified there under Accepted Digits, then 9 must also be entered here.

- **Play Message**

  Causes the desired message to be played. Any audio file present in the UC Suite can be selected. In addition, a new audio file can be imported into the UC Suite or a new announcement can be recorded and then imported as an audio file into the UC Suite.

  The playback of the announcement seizes one respective Media Stream channel.

  Properties:

  – **File Name**: Selection of an announcement (audio file in WAV format)
  – **Interrupt Digits**: specification of a key or key combination on the dial pad with which callers can stop the playback of an announcement.
  – **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.
- **Music on Hold**

  Causes Music on Hold (MOH of the communication system) to be played for external calls for an adjustable period of time

  Property:

  – **Time Value**: Time, in seconds, for which the Music on Hold is to be played.
- **Disconnect Caller**

  Causes the call to be disconnected.

  After this CCV object, no further CCV object may be inserted.
- **Play Queue Position**

  Causes information on the current queue position of the caller to be played.
- **Estimated Waiting Time**

  Causes information on the estimated waiting time of the caller to be played.

  The estimated waiting time is calculated based on:

  1) Historical average queue time for all queues
  2) Historical average queue time for the particular queue
  3) Historical average talk time for the particular agent
- **Go to CCV**

  Causes a loop to another CCV object

  Property:

  – **Target CCV**: Selection of the CCV object
- **Record Callback**

  Enables a caller in a queue to enable an agent callback (record a voicemail). Instead of the actual caller, the agent callback remains in the queue. For

agents with the **Enable agent callback** feature, the agent callback appears in the list of Contact Center calls.

After this CCV object, no further CCV object may be inserted.

Properties:

– **Type**: Selection of **Simple Callback** or **Extensive Callback**.

In contrast to simple callbacks, extensive callbacks offer callers additional options and information (e.g., the option to confirm or change the phone number that is to be called back and the option to confirm the voicemail).

– **Maximum message length**: Time, in seconds, that is available to a caller when recording a voicemail.

• **Process after digits**

Causes the next CCV object(s) to be executed, depending on the digits specified there (process digit).

Properties:

– **File Name**: Selection of one or more announcements (audio file in WAV format)
– **Playlist**: List of selected announcements (audio file in WAV format) in the order in which they are played
– **Digits Timeout**: Time, in seconds, for which the communication system waits for the input of digits.

If the required digits are not entered fully within the specified time, the message (announcement) is played again.

– **Link To**: List of digits with destination.

The digits and destinations can be added, edited and removed.

– **File Manager**: Using this button, it is possible to directly upload an audio file in wav format or create a new voice file with the recording device.

The contents of the Playlist are presented in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.

• **Single-step transfer**

This function depends on the **Normal Attendant Console SST** setting (WBM, **Expert mode**: **Applications** > **OpenScape Business UC Suite** > **Server** > **General Settings**):

– **Normal Attendant Console SST** enabled (default setting; not for U.S.): Causes the call to be transferred, regardless of whether the destination is free, busy or unavailable.

INFO: For stations with call waiting rejection enabled, the call is switched through only if the destination station is free. No call waiting on busy occurs.

– **Normal Attendant Console SST** disabled (default setting, only for U.S.): Causes the call to be transferred if the destination is free.

If the destination is busy and call waiting rejection is disabled, or if the destination is unavailable, an announcement is played back to the caller. The caller can then optionally choose to leave a message in the

voicemail box of the called subscriber or select the call number of another destination.

If the destination is busy and call waiting rejection is enabled, the call is not switched through.

After this CCV object, no further CCV object may be inserted.

Property:

– **Target Extension**: specification of the internal call number or external DID extension with the number of the CO trunk. Blanks, commas and other characters are not allowed.

The call number of the target extension is displayed in the CCV object.

NOTICE: After Single-Step-Transfer, the system disconnects the call after ringing for 5 minutes.

- **Transfer To Queue**

  Causes the call to be transferred to a queue.

  After this CCV object, no further CCV object may be inserted.

  Property:

  – **Queue**: Selection of the queue
- **Record In Mailbox**

  Causes the call to be sent to the desired voicemail box of a subscriber or a voicemail group

  After this CCV object, no further CCV object may be inserted.

  Property:

  – **User Mailbox**: specifies the station number of the voicemail box of a subscriber or voicemail group

  The station number and the name of the voicemail box or voicemail group are shown in the Rule Editor by a tool tip on hovering with the mouse pointer over the CCV object.
- **Supervised Transfer (also called screened transfer)**

  Causes the call to be transferred to an internal destination. During the transfer, Music on Hold (MOH of UC Suite) is played back to the caller.

  In contrast to the single-step transfer CCV object, two further CCV objects must be inserted here. This is because we now need to define how the communication system should behave if the call destination is busy or does

not answer the call. Usually, an announcement is played to the caller in such cases.

Properties:

– **Target Extension**: Specification of the internal phone number.

  Only internal call numbers are supported in the own node. Forwarding to external destinations, virtual stations, additional AutoAttendants, Mobility users, as well as external CallMe destinations, is not allowed!

  For these scenarios the SST (single-step transfer) should be used. To transfer a call to another UCD that is part of Contact Center, the CCV object **Transfer to Queue** should be used.

– **Ring Timeout**: Time, in seconds, within which the call must be accepted.

  If the call is not answered within the specified time, it is returned to the communication system, and the next CCV object is used.

  INFO: The time specified here must be shorter than the time configured for call forwarding (the default setting for call forwarding = 15 seconds). See How to Configure Call Forwarding.

– **Pull back call if destination device is forwarded / deflected**: Option (only applicable for internal call number.)

  If this option is enabled, the call destination is first checked, and if a forwarding destination or deflection has been set for it, the call is returned to communication system, and the next CCV object is used.

– **Check Presence status when transferring call**: Option

  If this option is enabled, the presence status of the call destination is checked, and if this status is any presence status other than Office, the call is returned to communication system, and the next CCV object is used.

• **Dial By Name**

  Causes the caller to be prompted to enter the first three letters of the desired subscriber's last name via the dial pad.

  If a unique subscriber name with the entered initial letters is found, a connection is established.

  If there are several subscriber names with the entered initial letters, these subscriber names are announced to the caller (max. 10 subscribers). If a subscriber has no recorded name announcement, the call number is announced instead. After selecting the desired subscriber, a connection is made.

  If none of the subscribers match the entered initial letters, the caller receives a corresponding message.

  INFO: The keys on the dialpad respond to the first press of a key. With each key pressed, the system tries to determine whether there are subscriber last names with the letter assigned to that key.

  Example: Let us assume the internal phone book has five last names with the initial letters t, u and v: Taylor, Taler,

Ullrich, Vasquez and Volterra. To establish a connection with the subscriber Taylor, following keys must be pressed: 8 2 9

After this CCV object, no further CCV object may be inserted.

Properties:

– **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.

Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions for which the first and last names of the subscriber are entered in the internal directory are supported here.

- **Dial By Extension**

Causes the caller to be prompted to enter the station number (extension) of the desired subscriber via the dial pad.

If the caller dials the station number of a virtual station, the caller is prompted to enter another station number. A connection is then established. If the desired subscriber does not respond, the call is accepted by his or her voicemail box.

After this CCV object, no further CCV object may be inserted.

Properties:

– **Method**: Selection of **Transfer To Extension** or **Record In Mailbox**.

Depending on the method selected, a connection to the desired extension or its voicemail box is established. Note that only internal extensions in the network for which the phone number is entered in the internal directory are supported here.

- **Set language**

Selects the language for each standard announcement based on the phone number of the caller. It should be noted that only standard announcements (i.e., system announcements) and no personal greetings are taken into account here.

For example, it is possible to have German announcements played back to callers with the country code +49 and French announcements for callers with the country code +33.

Properties:

– **Default language**: Drop-down list to select a language.

The language selected here is used for all phone numbers for which no specific language was defined.

– **Pattern**: Specifies the phone numbers to which a particular language is to be assigned.

The following placeholders can be used * = any digit, ? = any digit.

– **Language**: Drop-down list to select the language to be assigned to the relevant phone numbers (matching **Pattern**).

A language can be assigned to any number of different phone numbers (matching **Pattern**).

- **CLI Routing**

  Causes the forwarding of a call to one or more sequential CCV objects based on the caller's number.

  For example, it is possible to first have a German announcement played back to callers with the country code +49 (CCV object **Play Message**) and then have the call forwarded to an internal phone (CCV object **Single Step Transfer**). The area code can also be used (e.g. 089 for Munich).

  In the context of UC Suite and CLI Routing, users need to consider specific scenarios, such as incoming calls from MS Teams Native SIP Trunk. If you intend to send towards OpenScape Business caller's numbers in canonical format, including country code, then you have to establish additional CLI Routing rules.

  For example, if callers from MS Teams have numbers in the format +49777555XXXX, and 777555 is the common part of these numbers, users should create relevant CLI Routing rules that incorporate this common part (777555).

  Properties:

  – **Standard**: Drop-down list to select the CCV object.

    The CCV object selected here is used for all phone numbers for which no specific destination was defined.
  – **Pattern**: Specifies the phone numbers to which a specific CCV object is to be assigned as the destination.

    The following placeholders can be used * = any digit, ? = any digit.
  – **Description**

    Provides an explanation.

    For the **Pattern** +49 (= country code for Germany), for example, Germany can be entered.

    The text entered here will appear in the Rule Editor.
  – **Target**: Drop-down list to select the CCV object that is to be assigned as a destination to the related phone numbers (matching **Pattern**).

  A CCV object can be assigned as a destination to any number of different phone numbers (matching **Pattern**).
- **Branch on variable**

  Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.

  You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.

  Properties:

  – **Variable**: Selection of **Calls** or **Available agents**.

    Depending on the selected variable, the number of calls waiting in a queue or the number of available agents (including agents in wrap up time) is used as the defined condition. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to**

or greater than, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field.
  - **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
  - **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.

  The number of available agents in a queue is affected by the following status changes of the agents:

  - Login of an agent into the queue using "Anmelden/Login": --> +1
  - Logout of an agent from the queue using "Abmeldung/Logout": --> -1
  - Agent in the status "Break":-->-1
  - Agent in the status "Available after Break":--> +1

  The number of available agents in a queue is **not** affected by the following status changes of the agents:

  - Agent in the status "Ringing"
  - Agent in the status 'Talking'
  - Agent in the status "Wrap up"
  - Agent in the status "Missed Call"
  - Agent in the status "Overdue"
- **Branch on data**

  Causes the forwarding of a call to one or more sequential CCV objects based on a given condition.

  You can thus define, for example, that an announcement (such as "Please call again later ...") should be played back to callers as soon as there are more than 20 calls in a queue.

  Properties:

  - **Variable**: Selection of **LDAP data1 (xmpp)** or **LDAP data2 (pager)**.

    The data query is done via LDAP either directly to an LDAP capable database or indirectly via the Directory Service (ODS) to an SQL / ODBC database. The query results are assigned via the UC Suite LDAP field mapping to the appropriate criterias of the Contact Center. In the associated drop-down list, the condition (**less than**, **greater than**, **less than or equal to**, **equal to or greater than**, **equal to**) must be selected, and the comparison value must then be entered in the corresponding input field. It is necessary to map the keywords "pager" and "info".
  - **Timeout**: The time in seconds before a timeout occurs.
  - **Timeout branch**: Drop-down list to select the CCV object that is to be used as a destination when timeout occurs.
  - **True branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is satisfied.
  - **False branch**: Drop-down list to select the CCV object that is to be used as a destination when the condition is not satisfied.
  - **Description**: Provides an explanation.

18.3.3 Wrap up

Wrapup reasons can be used to assign incoming calls to specific categories (orders, complaints, service, etc.). The assignment is made by an agent after

completing the call (during the work time) by entering the appropriate wrapup reason using myAgent.

Wrapup reasons can be defined individually for each queue.

A distinction is made here between:

- Simple Wrapup

  One or more wrapup reasons can be defined for queues with the wrapup mode "Simple Wrapup".

  Example: The two wrapup reasons "hardware problem" and "software problem" were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the work time. This makes it possible to subsequently create a report with an overview of all calls related to the subject of hardware problems, for example.

- Multiple Wrapup

  For queues with the wrapup mode "Multiple Wrapup", one or more wrapup reasons can be defined and then classified into groups and subgroups.

  Below each group or subgroup (if any) at least one item should also be configured, to be able for the agent to wrapup a call. Wrapping a call up is not possible if a group or subgroup is empty. This applies only for queues which have Multiple Wrapup configuration enabled.

  Example: A Hardware group with the wrapup reasons Motherboard and Power Supply and a Software group with the wrapup reasons Operating System and Drivers were defined for a queue. Every call is assigned one of these wrapup reasons by an agent during the work time. This makes it possible to subsequently create a report with an overview of all calls related to hardware problems or also all calls related specifically to motherboard hardware problems.

18.3.4 Grade of Service

The Grade of Service can be used to assess the response rate of the queue. This is achieved by comparing the waiting time for callers in the queue with target values, which can be specified individually for each queue.

The target values for the Grade Of Service (GoS) can be defined freely, depending on the acceptable waiting time for callers in a queue. For each call to an appropriate queue, the service level is determined after the call and committed to the database. The Grade of Service can be evaluated by agents with the authorization level of a Supervisor or Administrator by using the myAgent application.

18.3.5 Wallboard

Queue details can be retrieved and displayed using myAgent. The display contains a table with statistical information on queues in real time for the current 24-hour period. The display can then be presented on a large LCD monitor, for example, or via a beamer (wallboard).

Agents with the agent authorization level receive information on the queues to which they are assigned. Agents with the Supervisor or Administrator authorization level receive information on all queues.

A separate station should be set up for a wallboard display. A Station license (IP User or TDM User) and a myAgent license are required for this.

18.3.6 Agent Callback

If the waiting time in the queue is too long for a caller, and the associated schedule includes the CCV object **Record Callback**, the caller can leave a callback request. This callback request retains the original position of the caller in the queue and is delivered to the agent in the form of a voicemail. After listening to the voice message, the agent can call back the caller via a screen pop.

If a preferred agent has been set for a caller, an attempt is first made to route the callback requests of that caller to the preferred agent. If the preferred agent is not available, the callback request is forwarded to any available agent.

18.4 VIP service

For each queue, you can individually define whether certain callers (with a VIP status) or callers which match configurable call number patterns should be given preferential treatment and thus allowed to reach a free agent faster.

If all agents of a queue are busy, VIP callers are preferentially connected to the next available agent.

18.4.1 VIP Caller Priority

The VIP Caller Priority can be defined individually for each queue in order to specify whether callers (customers, for example) included in the VIP Call List should be given preferential treatment.

The values for the VIP Caller Priority can be defined freely, depending on the waiting time for callers in a queue. This determines the level of preference for VIP callers as opposed to normal callers.

When a VIP caller activates an agent callback (by recording a voicemail with a callback request), the agent callback is retained in the queue instead of the VIP caller. but without the VIP Caller Priority.

VIP callers must be registered in the VIP call list directory (see VIP Call List).

18.4.2 VIP Call List

Callers who have already been registered in the communication system (external directory) can be added to the VIP call list. Multiple selection can be done or the "**Select All**" function can be used. In addition, call number patterns can be entered. A call number pattern consists of a specific sequence of digits

and a wildcard (placeholder). It can thus be used to transfer all employees of a company to the VIP call list, for example.

For each queue, the VIP caller priority can be used to define whether

- the callers included in the VIP call list and
- the callers who match the call number pattern contained in the VIP call list should be given preferential treatment.

It is not possible to enter call number patterns in the canonical call number format. The use of shortcut characters for country codes (for example +49 instead 0049) is likewise not possible. Call number patterns must always be specified without the CO access code.

Examples of call number patterns:

- 089 7577* (089 = area code for Munich, 7577 = PABX number of a company, * = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Munich, whose telephone number begins with 7577, are given priority.
- 0039* (0039 = country code for Italy, * = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Italy are given priority.

The following characters can be used as wildcards (placeholders) in a call number pattern:

- * = wildcard for any number
- ? = wildcard for any digit

18.5 Fallback solution

If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center.

In the event of a failure in the Contact Center, incoming calls are distributed according to the fallback solution. The distribution of faxes and e-mails is not possible.

Depending on requirements, one of the fallback solutions described below can be configured.

Default Fallback Solution

In this case, the fallback solution is based on the UCD IDs (agent IDs) of the agents:

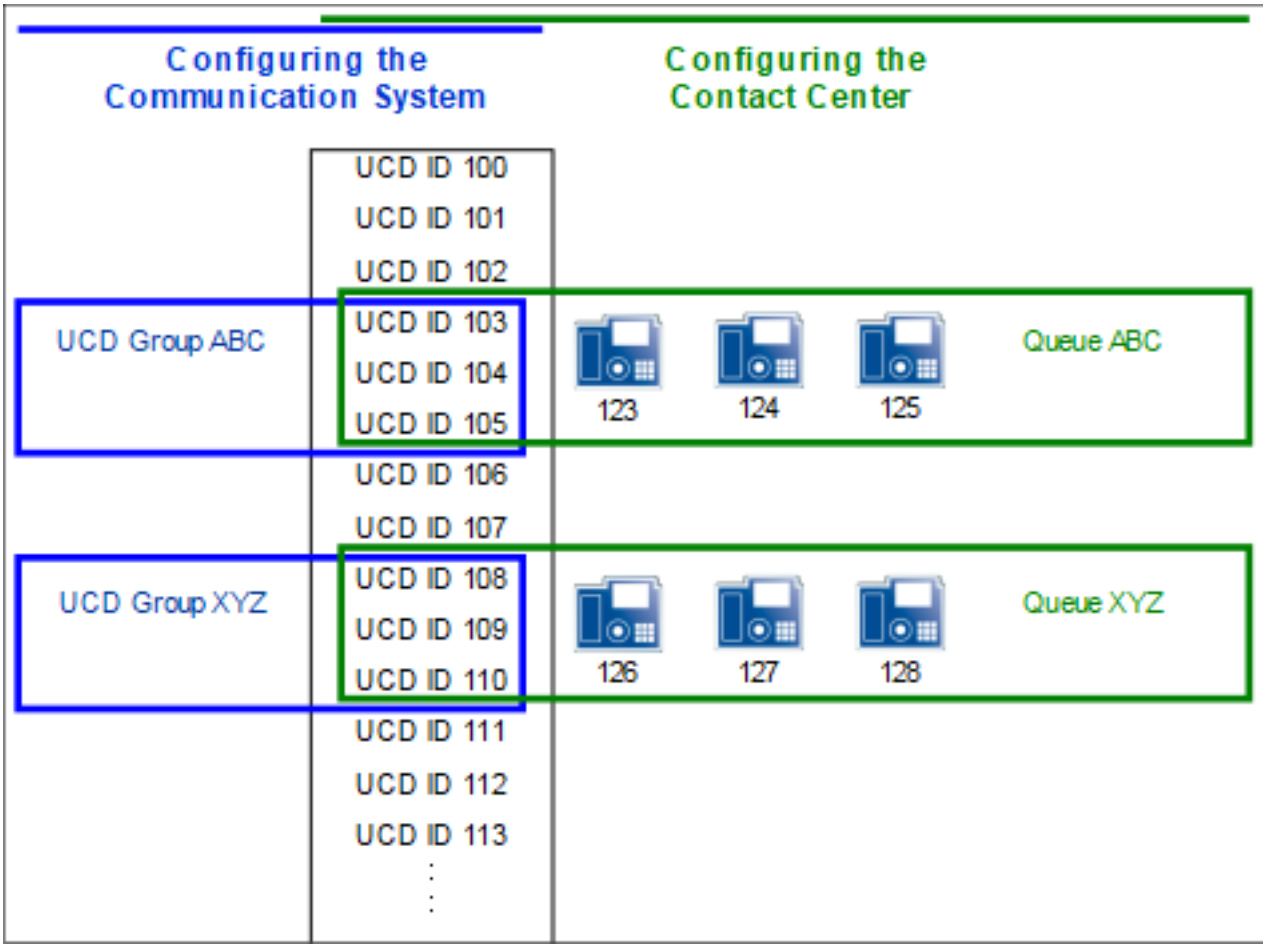
- Agents are assigned to the UCD groups of the communication system based on UCD IDs. The UCD ID determines to which UCD group this agent is assigned in the event of a failure at the Contact Center.

To ensure that the default fallback solution works properly, every queue must be assigned the Contact Center agents with the UCD IDs that were assigned to the appropriate UCD groups.

In the event of a failure in the Contact Center, incoming calls are distributed to the logged in agents via the different UCD groups.

Example:

- UCD IDs 103, 104 and 105 are assigned to UCD group ABC. UCD IDs 108, 109 and 110 are assigned to UCD group XYZ.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.
- When assigning agents to queues, the stations 123, 124 and 125 must be assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



Basic fallback solution

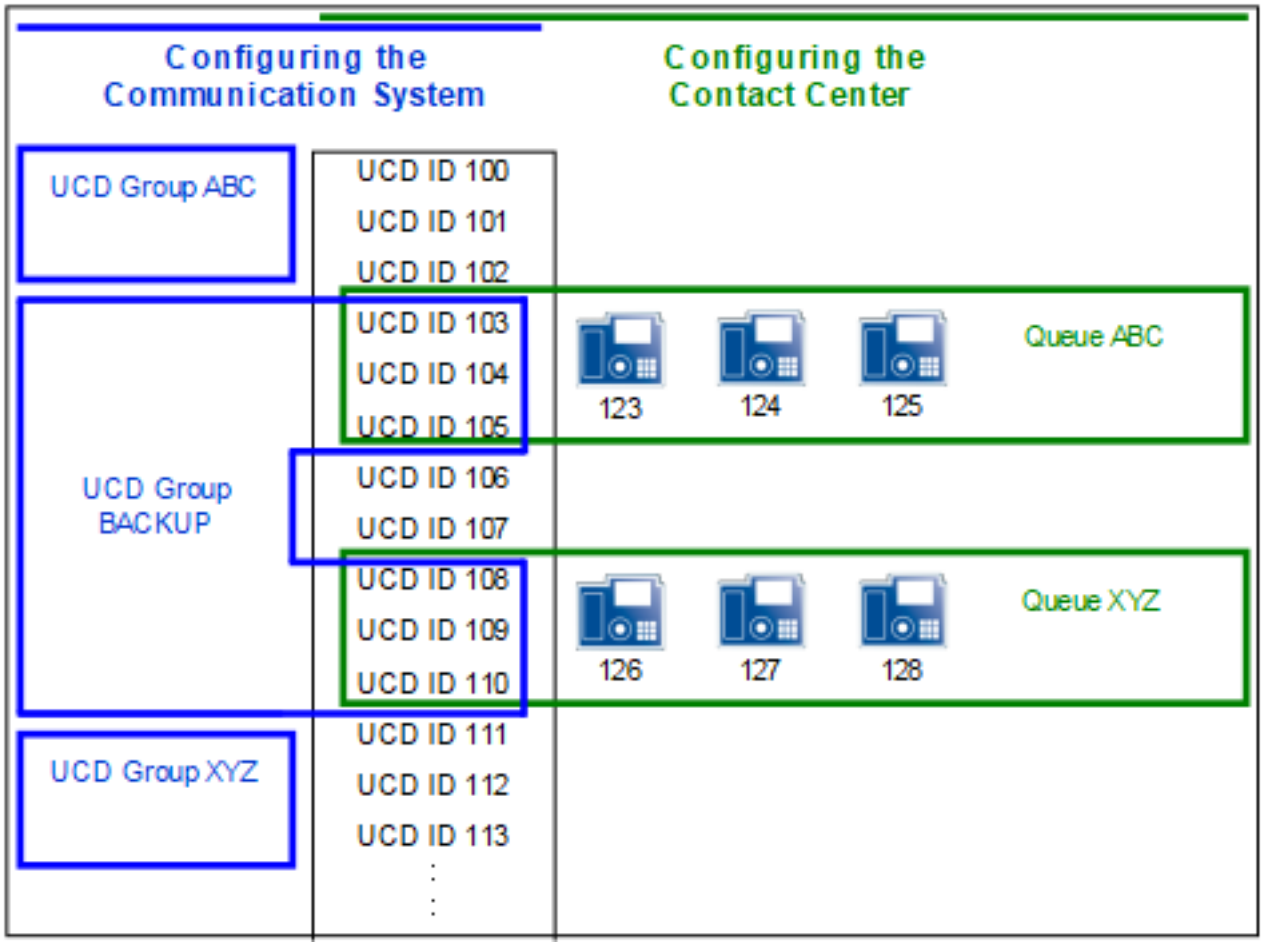
In this case, all agents of the Contact Center are assigned using their UCD IDs to only the Backup UCD group. By assigning the appropriate agents, these UCD IDs are then also used in the queues of the Contact Center. This ensures that in the event of a failure in the Contact Center, the agents do not have to manually log in at their phones with a different ID. This Backup UCD group is defined as a second call forwarding destination for all UCD groups of the communication system.

NOTICE: The configured Backup UCD group must also be configured as group into the Contact Center. This is the only way to ensure that this group is also monitored.

If the Contact Center fails, the incoming calls are then distributed to all agents of the backup UCD group.

Example:

- No UCD IDs were assigned to the UCD groups ABC and XYZ. UCD IDs 103 to 105 and 108 to 110 were assigned to the UCD group BACKUP.
- The stations 123, 124 and 125 are configured as agents with the UCD IDs 103, 104 and 105. The stations 126, 127 and 128 are configured as agents with the UCD IDs 108, 109 and 110.
- When assigning agents to queues, the stations 123, 124 and 125 are assigned to the queue ABC, and the stations 126, 127 and 128 to the queue XYZ.



Custom fallback solution

In this case, the customized configuration of the Contact Center is mapped via multiple UCD groups.

If the Contact Center fails, similar behavior is thus achieved by the fallback solution.

For details on configuring call distribution via the "Uniform Call Distribution (UCD)" feature of the communication system, see UCD (Uniform Call Distribution) .

The main advantage of the of the custom fallback solution, by contrast, lies in its accurate mapping of the Contact Center operations.

The disadvantage of the custom fallback solution is the high configuration effort involved. Furthermore, to achieve similar call distribution behavior, all

changes made to the Contact Center configuration also need to be mapped to the fallback solution.

The main advantage of the default and basic fallback solution is the easy configuration.

18.6 Configuring the Contact Center

When configuring the Contact Center, the UCD groups must be defined first. The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The actual configuration of the Contact Center (schedules, queues, etc.) can then be performed.

Before configuring the Contact Center, the standard processes for call distribution in normal and emergency modes must be coordinated with the customer.

INFO: The configuration of the Contact Center should only occur after the setup of the communication system and the UC suite have been fully completed.

If changes are made to the configuration of the UCD groups, then the UC Suite must be subsequently restarted via the Service Center of the WBM.

The following licenses are a prerequisite for the operation of a Contact Center:

- An appropriate number of licenses for agents (myAgent)
- Contact Center Fax License (for receiving and sending faxes), if necessary
- Contact Center E-mail License (for receiving and sending e-mails), if necessary

18.6.1 Example of a Contact Center Configuration

The operating principle of the Contact Center with OpenScape Business is presented here with the aid of an example. The structure and configuration of the example are based on a fictional customer scenario with standard Contact Center functions.

Sample Scenario for a Contact Center

Company XYZ operates a Contact Center with the following station numbers (queues):

- Station number 440 for the Service Department
- Station number 444 for the Sales department
- Station number 456 for free calls (Hotline). Callers receive an announcement and can then reach the Service or Sales Department by selecting the appropriate digit.

The Contact Center consists of six employees (agents), of which three work for the Service Department and three for Sales.

The queues for the Service and Sales Departments should be directly reachable during normal business hours from 09:00 to 17:00 hours. Both queues have a fax box and an e-mail address.

If all agents are busy or not available, callers are to be notified accordingly and have music played back to them. Is no agent becomes free after a certain period of time, a caller can leave a callback request or and reach the Attendant by dialing a specific number. If no digit is dialed, the caller should be automatically placed back in the queue.

During closed hours, callers are to hear an announcement enabling them to record a voicemail with a callback request (agent callback).

NOTICE: Playing announcements are only possible via trunks. In order to play the announcement the call must come from a trunk or the caller should be monitored by OpenScape Contact Center.

During the lunch break from 12:00 to 13:00 hours, an announcement is to be activated for the Service and Sales Departments to offer callers the option of recording a message with a callback request.

Fallback solution via Backup UCD group: If the Contact Center is unavailable due to problems (such as a system crash, dropped connection, etc.), the system should automatically switch to the "Uniform Call Distribution UCD" feature of the communication system as a fallback solution. This requires all of the Contact Center agents to be assigned to a single backup UCD group. For all UCD groups of the communication system, this Backup UCD group should be defined as a call forwarding destination. If the Contact Center fails, the incoming calls will then distributed to the agents of the Backup UCD group.

Configuring the Sample Scenario

The following actions must be performed for this sample scenario:

- Configure UCD groups

  The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.

  For this example of the Contact Center of company XYZ, three UCD groups (Service, Sales and Hotline) are to be configured.
- Configure the fallback solution

  For this example, a Backup UCD group is to be configured and defined as a call forwarding destination for all UCD groups of the communication system.
- Configure subscribers as agents

  For this example, six subscribers must be configured as agents.
- Record individual announcements

  For this example, various announcements are to be recorded. This includes an announcement for situations when no agent is available, for example, or an announcement to inform callers about possible options (using **Process after digits**).
- Load individual announcements

  For this example, the recorded announcements are to be loaded into the communication system.

- Define schedules

  For each time interval within a schedule, rules (Call Control Vectors or CCVs) can be defined to determine how incoming calls are to be handled on specific days and at specific times.

  In the example, a standard schedule XYZ is to be defined with a rule for the times outside business hours and with exceptions for business hours and the lunch break. In addition, a second schedule (Standard Schedule Hotline) to be defined with a rule for free calls (Hotline).

Schedule	Rule (CCV)	
Standard Schedule XYZ	Out of the Office	Times outside business hours
	Open	Business hours 08:00 to 11:59 hours = Open1
		Business hours 13:00 to 17:00 hours = Open2
	Lunch Break	Lunch 12:00 to 12:59 hours
Standard Schedule Hotline	Hotline	24 Hours

- Adding three queues

  In this example, one queue is to be configured for the Service Department and one for Sales. A further queue (hotline) is to be configured for free calls.

- Assign agents to queues

  For this example, three agents are to be assigned to the Service queue and three to the Sales queue.

More details on the configuration of all Contact Center functions can be found under the Configuration Procedure .

18.6.1.1 How to Configure UCD Groups for the Sample Contact Center

This example shows you how to use the **UCD** wizard to define the three UCD groups (Service, Sales and Hotline) with the station numbers 440, 444 and 456 for the sample Contact Center of company XYZ.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **User Telephony**.

3) Click on **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.

4) To configure a UCD group, click **Edit** in the row containing the required UCD group.

5) Enter the call number `440` of the Service UCD group in the **Call number** field.

6) Enter the DID number `440` of the Service UCD group in the **Direct inward dialing number** field.

7) Enter the name **Service** in the `Name` field.
8) Click on **OK & Next**. The window **Assignment of UCD Agents** is displayed.
9) Click on **OK & Next**, since no UCD IDs may be assigned for the UCD group Service.

   Since a fallback solution via a Backup UCD group is to be set up for the sample Contact Center of company XYZ, no UCD IDs should be assigned to the three UCD groups Service, Sales, and Hotline.
10) Click on **OK & Next**. The **Edit announcement/overflow** window appears.
11) Click on **OK**, since the displayed parameters are not relevant for the configuration of the UCD group.
12) Repeat steps 4 through 11 for the UCD group Sales with the call number 444 and for the UCD group Hotline with the call number 456.
13) Click on **OK & Next**, followed by **Finish**.

18.6.1.2 How to Configure a Fallback Solution for the Sample Contact Center

You can configure the Backup UCD group with the call 400 for the sample Contact Center of company XYZ with **UCD** wizard. In the example, the UCD agent IDs 101 to 106 are used. In addition, you will define the Backup UCD group as a call forwarding destination for all UCD groups of the sample Contact Center of company XYZ.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

The Backup-UCD group with the call number 400 needs to be configured in the UC Suite Contact Center queues.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.
4) To configure a UCD group, click **Edit** in the row containing the required UCD group.
5) Enter the call number `400` of the UCD group Backup in the **Call number** field.
6) Enter the DID number **400** of the UCD group Backup in the `Direct inward dialing number` field.
7) Enter the name `Backup` in the **Name** field.
8) Click **OK & Next**. The window **Assignment of UCD Agents** is displayed.
9) Mark the required UCD agent IDs in the **Selection** and assign them to the UCD group Backup by clicking **Add**.
10) Click **OK & Next**. The **Assign stations** window appears.
11) Assign the desired stations to all UCD agent IDs.
12) Click **OK & Next**. The **Edit announcement/overflow** window appears.
13) Click **OK**, since the displayed parameters are not relevant for the configuration of the UCD group Backup.

14) To configure the new Backup UCD group as a call forwarding destination for the UCD group Service, click in the row of the UCD group Service on **Edit**.
15) Click **OK & Next** until the **Edit announcement/overflow** window appears.
16) Select the UCD group Backup with the call number 400 as the call forwarding destination in the **Overflow destination** drop-down list.
17) Click **OK**.
18) Repeat steps 14 through 17 to configure the new UCD group Backup as the call forwarding destination for the UCD groups Sales and Hotline, respectively.
19) Click on **OK & Next** followed by **Finish**.

18.6.1.3 How to Configure a Subscriber as an Agent for the Sample Contact Center

This example shows you how to use the **User Directory** wizard to configure subscribers as agents for the sample Contact Center of company XYZ. In the example, the subscribers with the station numbers 101 to 106 are configured as agents. The subscribers with the station numbers 101 and 104 are assigned the **Supervisor** authorization level, and the other subscribers are assigned the authorization level of an **Agent**.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard.
4) Mark the subscriber with the **Extension** 101 and click **Edit**.
5) Click in the menu tree on **Personal Details** > **User Level**.
6) Select the **Permanently available agent** check box. The agent will then remain available for calls, faxes and e-mails even when he or she does not accept a call, fax or e-mail.
7) Select the **Supervisor** authorization level in the **Level** drop-down list.
8) Click **Save**.
9) Repeat steps 4 through 8 to configure the subscribers with the station numbers 102 to 106 as agents.

18.6.1.4 How to Add Announcements for the Sample Contact Center

You can record announcements for the sample Contact Center of company XYZ with the **Recorder** wizard. Among other things, an announcement is needed for situations in which all agents are unavailable.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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**. The selected station number is called.
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.

INFO:

After the announcement has been recorded and saved, it can no longer be deleted. However, it can be overwritten by saving another file with the same file name. 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 How to Load Announcements for the Sample Contact Center

You can upload announcements for the sample Contact Center of company XYZ with the **File Upload** wizard.

Prerequisites

An audio file in .wav format is available with the following properties: mono, audio sample rate 8 kHz, audio sample size 16 bit, frame size 2.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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**.

INFO:

After the audio file is uploaded, it can no longer be deleted. However, it can be overwritten by uploading another file with the same file name. 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 How to Add the Standard Schedule XYZ for the Sample Contact Center

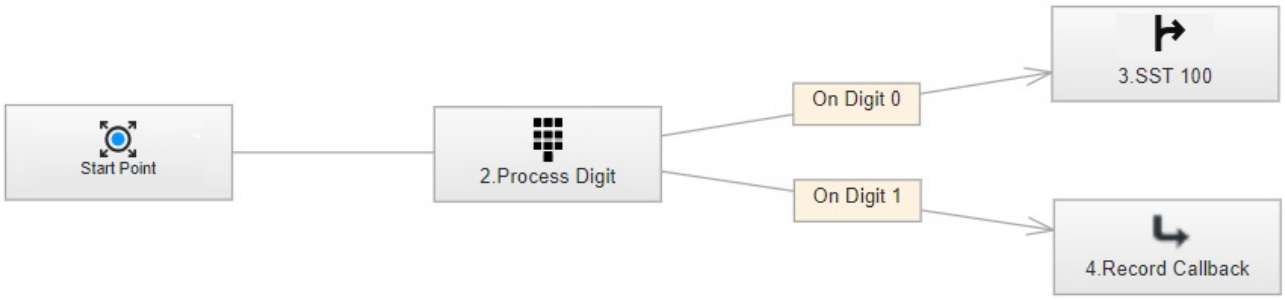
This example shows you how to use the **Contact Center** wizard to define a schedule with rules for breaks and business hours for the sample Contact Center of company XYZ. In the example, a schedule (Standard Schedule XYZ) is to be defined with a rule for the times outside business hours (Out of the Office) and exceptions for the business hours (08:00 to 11:59 hours = Open1, 13:00 to 17:00 hours = Open2) and the lunch break (12:00 to 12:59 hours = Lunch Break).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
5) Click on **Add**.
6) Click on **Add** under the **Schedule** area.
7) Define the new mapped rule for times outside business hours.



Click in the list of CCV tools on one of the CCV objects contained in the displayed rule and drag it into the Rules Editor. Enter the properties indicated below in the window of the CCV object that appears and confirm this by clicking **Save**. Repeat the procedure for any additional CCV objects. Connect the CCV objects by clicking the right mouse button on the first of the two CCV objects to be joined. Then select the second of the two CCV

objects to be connected in the drop-down menu via **Link To**. Repeat the procedure for any additional CCV objects to be joined.

Property		Value
1st. CCV object: **Process Digit**		
	Playlist	Audio file in wav format
	Digits Timeout	5
	Description	Announcement: "Press digit 0 to ...; Press digit 1 to ...
2nd. CCV object: **Single Step Transfer**		
	Target Extension	100
	Description	Forward to Attendant Console
	Process after digits	0
3rd CCV object: **Record Callback**		
	Type	Extensive Callback
	Maximum message length	20
	Description	Callback request (Agent callback)
	Process after digits	1

Click on **Save ...**. Enter `Out of the Office` as the **CCV Name** of the rule and then click **Save**. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor. Close the window confirming that the rule was saved.

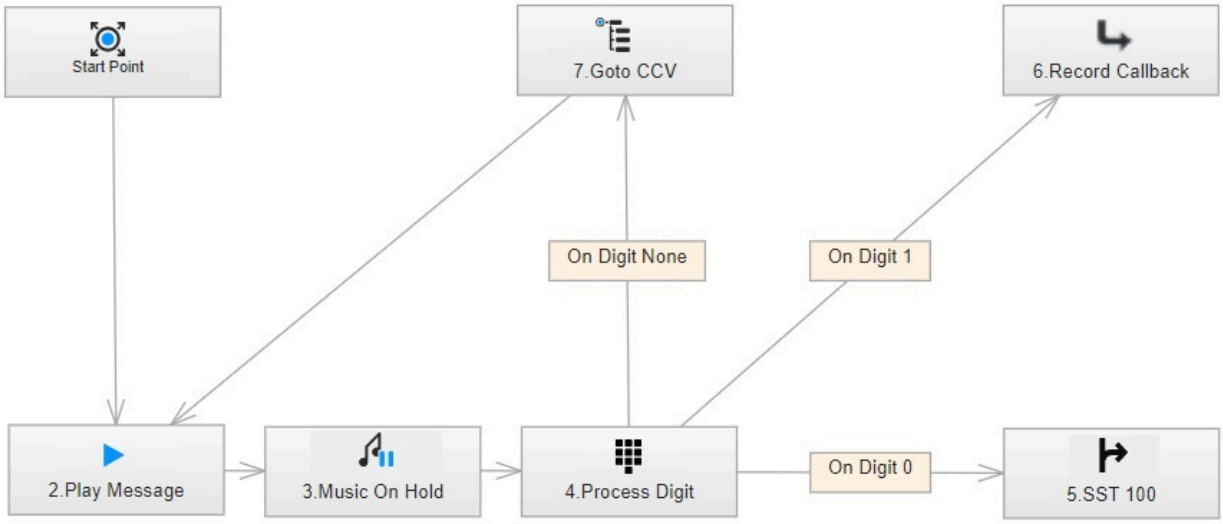
Select the rule `Out of the Office` in the **Default CCV** drop-down list.

8) Enter the name `Standard Schedule XYZ` in the **Schedule Name** field.

9) Click on **Save**.

10) Click on **Add** under the **Schedule** area.

11) Define the mapped rule for the business hours.



Click in the list of CCV tools on one of the CCV objects contained in the displayed rule and drag it into the Rules Editor. Enter the properties indicated below in the window of the CCV object that appears and confirm this by clicking **Save**. Repeat the procedure for any additional CCV objects. Connect the CCV objects by clicking the right mouse button on the first of the two CCV objects to be joined. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**. Repeat the procedure for any additional CCV objects to be joined.

Property	Value
1st. CCV object: **Play Message**	
File name	Audio file in wav format
Interrupt digits	5
Description	Agent not available announcement
2nd. CCV object: **Music on Hold**	
Time value	30
Description	Music on Hold for 30 seconds
3rd. CCV object: **Process Digit**	
Playlist	Audio file in wav format
Digits Timeout	5
Description	Announcement: "Press digit 0 to ...; Press digit 1 to ...
4th. CCV object **Single Step Transfer**	
Target Extension	100
Description	Forward to Attendant Console
Process after digits	0

Property	Value
5th. CCV object: **Record Callback**	
Type	Extensive Callback
Maximum message length	20
Description	Callback request (Agent callback)
Process after digits	1
6th. CCV object: **Go to CCV**	
Target CCV	1. Play Message
Description	Back to announcement

Click on **Save ...**. Enter `Open` as the **CCV Name** for the new rule and then click **Save**. Close the window confirming that the rule was saved.

In the drop-down list, select the rule `Open` for the Open1 exception.

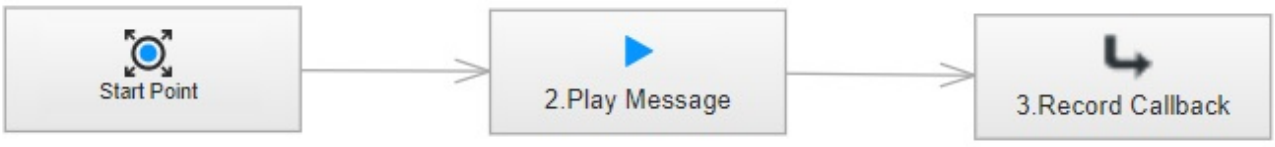
12) In the **Exceptions** area, click on **Add** to define the first exception for business hours.
13) Enter **Open1** in the `Description` field.
14) Define at what time the exception Open1 is to apply:

    Enable the **Within time range** radio button. Select **08:00** as start time in the `Start Time` list box and **11:59** as end time in the `End Time` list box to define the daily time period.

    Select the weekdays on which the rule is to be applied in the **Select days** window. Then click **Save**.
15) In the **Exceptions** area, click on **Add** to define the second exception for business hours.
16) Enter `Open2` in the **Description** field.
17) In the drop-down list, select the rule `Open` for the Open2 exception.
18) Define at what time the exception Open2 is to apply:

    Select the **Within time range** from the **Type** drop-down list. Select **13:00** as start time in the `Start Time` list box and **17:00** as end time in the `End Time` list box to define the daily time period.

    Select the weekdays on which the rule is to be applied in the **Select days** window. Then click **Save**.
19) Define the mapped rule for the lunch break.



Click in the list of CCV tools on one of the CCV objects contained in the displayed rule and drag it into the Rules Editor. Enter the properties indicated below in the window of the CCV object that appears and confirm this by clicking **Save**. Repeat the procedure for any additional CCV objects. Connect the CCV objects by clicking the right mouse button on the first of the two CCV objects to be joined. Then select the second of the two CCV

objects to be connected in the drop-down menu via **Link To**. Repeat the procedure for any additional CCV objects to be joined.

Property	Value
1st. CCV object: **Play Message**	
File name	Audio file in wav format
Interrupt digits	Select service
Description	Agent not available announcement
2rd CCV object: **Record Callback**	
Type	Extensive Callback
Maximum message length	20
Description	Callback request (Agent callback)
Process after digits	1

Click on **Save ...**. Enter `Lunch Break` as the **CCV Name** of the rule. Close the window confirming that the rule was saved.

In the drop-down list, select the rule `Lunch Break` for the Lunch Break exception.

20) In the **Exceptions** area, click on **Add** to define the exception for lunch break.

21) Enter **Lunch Break** in the `Description` field.

22) Define at what time the exception Lunch Break is to apply:

Select the **Within time range** from the **Type** drop-down list. Select `12:00` as the start time in the **Start Time** list box and `12:59` as the end time in the **End Time** list box to define the daily time period.

Select the weekdays on which the rule is to be applied in the **Select days** window. Then click **Save**.

23) If you want to test which rule (CCV) of the schedule is executed at a particular point in time, click on **Test Schedule**. Select the desired date and time in the **Date** and **Time** list boxes, respectively. Then click on **Test Schedule**. You will then be shown which rule (CCV) applies on that day and at that time. Click on **Close** to close the **Test Schedule** window.

24) Click on **Save**.

25) Close the window.

18.6.1.7 How to Add the Standard Schedule Hotline for the Sample Contact Center

You can define the schedule with a rule for free calls (Hotline) for the sample Contact Center of company XYZ with the **Contact Center** wizard.

Prerequisites

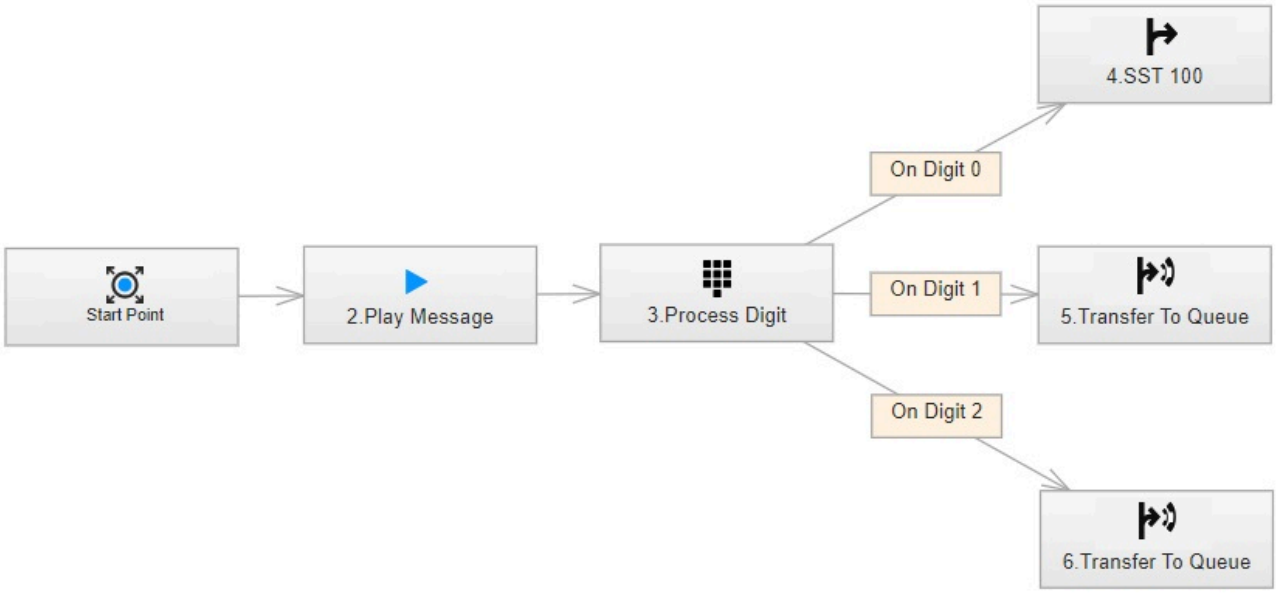
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
5) Click on **Add**.
6) Click on **Add** under the **Schedule** area.
7) Define the displayed rule for free calls (Hotline).



Click in the list of CCV tools on one of the CCV objects contained in the displayed rule and drag it into the Rules Editor. Enter the properties indicated below in the window of the CCV object that appears and confirm this by clicking **Save**. Repeat the procedure for any additional CCV objects. Connect the CCV objects by clicking the right mouse button on the first of the two CCV objects to be joined. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**. Repeat the procedure for any additional CCV objects to be joined.

Property	Value
1st. CCV object: **Play Message**	
File name	Audio file in wav format
Interrupt digits	5
Description	Announcement: Greeting
2nd. CCV object: **Process Digit**	
Playlist	Audio file in wav format
Digits Timeout	5
Description	Announcement: "Press digit 0 to ...; Press digit 1 to ...
3rd. CCV object: **Single Step Transfer**	
Target Extension	100
Description	Forward to Attendant Console

Property		Value
	Process after digits	0
4th. CCV object **Transfer To Queue**		
	Queue	440
	Description	Proceed to the Service queue
	Process after digits	1
5th. CCV object **Transfer To Queue**		
	Queue	444
	Description	Proceed to the Sales queue
	Process after digits	2

Click on **Save ...**. Enter `Hotline` as the **CCV Name** for the rule and then click **Save**. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor. Close the window confirming that the rule was saved.

Select the rule **Hotline** in the `Default CCV` drop-down list.

8) Enter the name `Standard Schedule Hotline` in the **Schedule Name** field.
9) Click on **Save Schedule**.

18.6.1.8 How to Add Queues for the Sample Contact Center

This example shows you how to use the **Contact Center** wizard to configure queues for the sample Contact Center of company XYZ. In the example, one queue is to be configured for the Service Department (with station number 440) and one for the Sales Department (with station number 444). A further queue (Hotline, station number 456) is to be configured for free calls.

Prerequisites

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.

At least one e-mail account is available for receiving e-mails.

The sending of e-mails has been configured in the communication system.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Queue**.
5) Click on **Add**.
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.

    If there are more than 20 calls waiting in the queue, the queue symbol at the agent changes from green to orange.
13) In the **Queue Alarm Time** field, enter the value `300`, for example.

    Once the waiting time for a queued call specified exceeds 300 seconds, the corresponding item in the list of Contact Center calls for the agents changes to red.
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`. This causes calls abandoned after 120 seconds to be included in the statistics (of a report).
16) Select the check box **Screen Pop Enabled**. A screen pop for displaying and entering customer data will then appear on receiving incoming calls 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.

    Faxes to these phone number/s will then be added to the queue and treated as incoming calls.
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).

Select whether e-mails are to be sent via an SSL (Secure Socket Layer) connection. If you want to use an SSL connection, select the **Use SSL connection** check box. (Note that the port number of the E-mail server may be changed as a result. The default port number for POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

Click on **Save**. 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) Click on **Save**.

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 How to Assign Agents to Queues of the Sample Contact Center

This example shows you how to use the **Contact Center** wizard to assign agents to the queues of the sample Contact Center of company XYZ. In the example, three agents of the Service queue and three agents of the Sales queue are assigned.

Prerequisites

The **Service** and **Sales** queues for the sample Contact Center have been set up.

Six agents were configured for the sample Contact Center.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click on **Edit** to start the **Contact Center** wizard.

4) Click on **Queue Bindings**. The **Service** and **Sales** queues are displayed.

5) Select queue to which you want to assign an agent and click on **Edit**. All agents already assigned are displayed.

6) Select the first agent for the **Service** queue from the table and click on **Edit**. The **Edit** window is then displayed.

7) Select one of the following options:
   - If the agent is to receive calls without regard to the load on the **Service** queue, select the **Primary Agent** from the **Type** drop-down list.
   - If the agent is to receive calls only when the **Service** queue overflows, select the **Overflow Agent** from the **Type** drop-down list.
8) If you have selected **Overflow Agent**:
   a) Enter the time after which incoming calls for an agent should be forwarded in an overflow situation in the **Overflow after seconds in queue** field.
   b) Enter the maximum number of calls in the **Overflow after calls in queue** field. Calls that exceed this maximum number are received by an overflow agent.
9) Enter a percentage value for the **Skill Level** of the agent.

   Skill levels enable you to control the distribution of calls to agents in the **Service** queue. Agents with higher skill levels are given preference during the call distribution. In cases where all agents have the same skill level, the longest idle agent receives the call.
10) Select one of the following options:
   - If the agent is to receive callback requests in the form of voice messages, select the check box **Enable agent callback**.
   - If the agent is to be prevented from receiving callback requests, clear the **Enable agent callback** check box.
11) Enter the automatic work time in seconds for the agent of the **Service** queue in the **Work Time** field.
12) Click on **OK**.
13) Repeat steps 5 through 12 to assign all agents to the queues of the sample Contact Center.

18.6.2 Configuration Procedure

This section contains an overview of the actions to be performed when configuring the Contact Center.

- Configure UCD groups

  The queues of the Contact Center are essentially workgroups that are based on the UCD groups of the communication system. The UCD groups must be defined before the actual configuration of the Contact Center.
- Configure a fallback solution

  If the Contact Center is unavailable due to problems (crash, connection down, etc.) the "Uniform Call Distribution (UCD)" feature of the communication system is automatically used. This feature thus serves as the fallback solution for the Contact Center (see Fallback solution).
- Configure subscribers as agents
- Record individual announcements for the Contact Center
- Load individual announcements for the Contact Center

NOTICE: Playing announcements are only possible via trunks. In order to play the announcement the call must come

from a trunk or the caller should be monitored by OpenScape Contact Center.

- Add schedules
- Add queues
- Define target values for the Grade of Service
- Define the VIP caller priority
- Edit the VIP call list
- Define preferred agents
- Add Contact Center breaks
- Add wrap-up codes
- Assigning agents to queues

18.6.2.1 How to Configure UCD Groups for the Contact Center

You can configure UCD groups for the Contact Center with the **UCD** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **UCD** wizard. The list of all possible UCD groups is displayed.
4) To configure a UCD group, click **Edit** in the row containing the required UCD group.
5) Enter the call number of the new UCD group in the **Call number** field.
6) Enter the DID number of the new UCD group in the **Direct inward dialing number** field.
7) Enter the name of the UCD group in the **Name** field.
8) Click **OK & Next**. The window **Assignment of UCD Agents** is displayed.
9) Mark the required UCD agent IDs in the **Selection** and assign them to this UCD group by clicking **Add**.
10) Click **OK & Next**. The **Assign stations** window appears.
11) Assign the desired stations to all UCD agent IDs.
12) Click **OK & Next**. The **Edit announcement/overflow** window appears.
13) Click **OK**, since the displayed parameters are not relevant for the configuration of the UCD group.
14) If you want to configure further UCD groups for the contact center, repeat steps 4 through 11.
15) Click **OK & Next**, followed by **Finish**.

18.6.2.2 How to Configure a Subscriber as an Agent

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard.
4) Mark the desired station in the user directory and click **Edit**.
5) Click in the menu tree on **Personal Details** > **User Level**.
6) Select one of the following options:

   If the agent is to be permanently available, select the **Permanently available agent** check box. The agent will then remain available for calls, faxes and e-mails even when he or she does not accept a call, fax or e-mail.

   If the agent is not to be permanently available, clear the **Permanently available agent** check box. The agent will then be assigned the status Unavailable when he or she does not accept a call, fax or e-mail.
7) Select the authorization level in the **Level** drop-down list.
8) Click **Save**.
9) If you want to configure another subscriber as an agent, repeat steps 4 through 8.

18.6.2.3 How to Record Custom Announcements for the Contact Center

You can record custom announcements for the Contact Center with the **Recorder** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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**. The selected station number is called.
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.

INFO:

After the announcement has been recorded and saved, it can no longer be deleted. However, it can be overwritten by saving another file with the same file name. For example,

saving an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

18.6.2.4 How to Load Custom Announcements for the Contact Center

You can load custom announcements for the Contact Center with the **File Upload** wizard.

Prerequisites

An audio file in .wav format is available with the following properties: mono, audio sample rate 8 kHz, audio sample size 16 bit, frame size 2.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **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**.

INFO: After the audio file is uploaded, it can no longer be deleted. However, it can be overwritten by uploading another file with the same file name. For example, uploading an audio file named `announcement1.wav` would overwrite any existing `announcement1.wav` file.

18.6.2.5 How to Add a Schedule

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
5) Click on **Add**.

6) Select one of the following options for choosing the rule (CCV):

- If you want to assign a previously defined rule to the schedule, select the desired rule in the **Default CCV** drop-down list.
- If you want to assign a new rule that has not yet been defined to the schedule click on **Edit** under the **Schedule** area and proceed as follows:

  Click in the list of CCV tools on the desired CCV object and drag it into the Rule Editor. Enter the desired properties in the window of the CCV object that appears and click **Save**. If required, drag further CCV objects into the Rule Editor and define their properties. To connect two CCV objects, right-click with the mouse on the first of the two CCV objects to be connected. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**.

  If you want to delete a CCV object from the Rule Editor, right-click on that CCV object and select **Remove** in the drop-down menu.

  Click on **Save ...**. Enter a name for the new rule and then click **Save**. Close the window confirming that the rule was saved. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor.

  Select the new rule just saved from the **Default CCV** drop-down list.
- If you want to assign a new rule that is based on a previously defined rule to the schedule, proceed as follows:

  Select the desired rule from the **Default CCV** drop-down list and click **Edit**. The rule will be displayed in the Rule Editor. Edit the rule.

  Click in the list of CCV tools on the desired CCV object and drag it into the Rule Editor. Enter the desired properties in the window of the CCV object that appears and click **Save**. If required, drag further CCV objects into the Rule Editor and define their properties. To connect two CCV objects, right-click with the mouse on the first of the two CCV objects to be connected. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**.

  Click on **Save ...**. Enter a **CCV Name** for the new rule and then click **Save**. Close the window confirming that the rule was saved. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor.

  Select the new rule just saved from the **Default CCV** drop-down list.

7) If you want to print the rule or send it via an e-mail, you can save the rule as a PDF file. To do this, click **Print**. The **Print** window appears.

Enter the name of the file and then select the directory in which the file is to be stored. Click on **Save**.

8) Enter the name of the new schedule in the **Schedule Name** field.

9) Click on **Save**.

10) If you want to assign another rule (CCV) for a specific time period within the schedule, click on **Add** in the **Exceptions** area. The fields for this exception will then be displayed.

11) Enter the name of the exception in the **Description** field.

12) Select one of the following options for choosing the rule (CCV):

- If you want to assign a previously defined rule to the time period within the schedule, select the desired rule from the drop-down list for this exception.
- If you want to assign a new rule that has not yet been defined to the time period within the schedule, proceed as follows:

  Click on **Add** under the **Schedule** area.

  Click in the list of CCV tools on the desired CCV object and drag it into the Rule Editor. Enter the desired properties in the window of the CCV object that appears and click **Save**. If required, drag further CCV objects into the Rule Editor and define their properties. To connect two CCV objects, right-click with the mouse on the first of the two CCV objects to be connected. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**.

  If you want to delete a CCV object from the Rule Editor, right-click on that CCV object and select **Remove** in the drop-down menu.

  Click on **Save ...**. Enter a name for the new rule and then click **Save**. Close the window confirming that the rule was saved. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor.

  Select the new rule just saved for this exception from the drop-down list.
- If you want to assign a new rule that is based on a previously defined rule to the time period within the schedule, proceed as follows:

  Select the desired rule from the drop-down list for this exception and click **Edit**. The rule will be displayed in the Rule Editor. Edit the rule.

  Click in the list of CCV tools on the desired CCV object and drag it into the Rule Editor. Enter the desired properties in the window of the CCV object that appears and click **Save**. If required, drag further CCV objects into the Rule Editor and define their properties. To connect two CCV objects, right-click with the mouse on the first of the two CCV objects to be connected. Then select the second of the two CCV objects to be connected in the drop-down menu via **Link To**.

  Click on **Save ...**. Enter a name for the new rule and then click **Save**. Close the window confirming that the rule was saved. If the new rule is invalid, it cannot be saved. The invalid CCV object is marked red in the Rule Editor.

  Select the new rule just saved for this exception from the drop-down list.

13) Select one of the following options to define at what time the exception is to apply:

- If the exception is to apply for an unlimited time period throughout the year, select the **Within time range** from the **Type** drop-down list. Select the start and the end of the daily time period in the **Start Time** and **End Time** list boxes.

  Select the weekdays on which the exception is to be applied. Then click **Save**.
- If the exception is to apply for a limited time period during the year, select the **Within time date range** from the **Type** drop-down list. Enter the starting and the ending dates for the time period during the year (format dd.mm.yyyy) in the **Start Date** and **End Date** fields,

respectively. Select the exact time of the start date and the exact time of the end date in the **Start Time** and **End Time** list boxes. The exception will apply between start date/start time to end date/end time of the covered period.

Select the weekdays on which the exception is to be applied. Then click **Save**.

- If the exception is to apply on holidays, select the **Holiday Schedules** from the **Type** drop-down list. Enter the starting and ending dates for the holiday schedule in the **Start Date** and **End Date** fields, respectively. Select the starting and ending times for the holiday schedule in the **Start Time** and **End Time** list boxes, respectively.

  INFO: Holiday schedules have precedence over the other schedules and rules of a queue.

- If the exception is to apply every year, select the **Yearly Recurrence** from the **Type** drop-down list. Enter the starting and ending dates for the yearly recurrence in the **Start Date** and **End Date** fields, respectively. Select the starting and ending times for the yearly recurrence in the **Start Time** and **End Time** list boxes, respectively.

14) Click on **Save**.

15) Repeat steps 10 through 14 if you want to define additional exceptions for specific time periods.

16) If you want to test which rule (CCV) of the schedule is executed at a particular point in time, click on **Test Schedule**. Select the desired date and time in the **Date** and **Time** list boxes, respectively. Then click on **Test Schedule**. You will then be shown which rule (CCV) applies on that day and at that time. Click on **Close** to close the **Test Schedule** window.

17) If you want to assign this schedule to one or more queues select the check box(es) for the desired queue(s) in the **Queues** area.

NOTICE: A selected Queue can only be assigned to one Schedule, but several different Queues can be assigned to a selected Schedule.

18) Close the window.

18.6.2.6 How to Edit a Schedule

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click on **Edit** to start the **Contact Center** wizard.

4) Click on **Schedule**. All existing schedules are displayed.

5) Mark the schedule to be edited and click **Edit**.

6) Change the desired settings for the default CCV:

- If you want to assign some other rule (CCV) than the one currently displayed in the **Default CCV** drop-down list, select the desired rule in the **Default CCV** list.
- If you want to edit the rule (CCV) shown in the **Default CCV** list, **Edit** under the **Schedule** area. The rule will be displayed in the Rule Editor. Edit the rule. Click on **Save ...**. Enter a name for the new rule and then click **Save**. Close the window confirming that the rule was saved.

  Select the new rule just saved from the **Default CCV** drop-down list.

7) Click on **Save**.

8) Change the desired settings in the **Exceptions** area:

- If you want to assign another rule (CCV) to a specific time period within the schedule, click **Add** under the **Exception** area. Select the desired rule in the drop-down list for this exception. Then use the radio buttons and drop-down lists to specify when this exception is to apply. Enter the name of the exception in the **Description** field. Click on **Save**.
- If you want to edit this exception or one of the exceptions displayed, click on the **Edit** under the **Exception** area after the selection of the desired exception and then use radio buttons, drop-down lists, fields to specify when this exception is to apply and on which rule (CCV). Additionally you can click on **Edit CCV** under the **Exception** area to edit the associated rule (CCV). The rule will be displayed in the Rule Editor. Edit the rule. Click on **Save ...**. Enter a name for the new rule and then click **Save**. Close the window confirming that the rule was saved.

  Select the new rule just saved from the drop-down list. Then use the radio buttons and drop-down lists to specify when this rule (CCV) is to apply. Click on the green Save icon.
- If you want to delete this exception or one of the exceptions displayed, click on the **Remove** after the selection of the desired exception.

9) If you want to test which rule (CCV) of the schedule is executed at a particular point in time, click on **Test Schedule**. Select the desired date and time in the **Date** and **Time** list boxes, respectively. Then click on **Test Schedule**. You will then be shown which rule (CCV) applies on that day and at that time. Click on **Close** to close the **Test Schedule** window.

10) If you want to assign this schedule to one or more queues select the check box(es) for the desired queue(s) in the **Queues** area.

NOTICE: A selected Queue can only be assigned to one Schedule, but several different Queues can be assigned to a selected Schedule.

---

11) Close the window.

18.6.2.7 How to Delete a Schedule

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All available schedules are displayed.
5) Mark the desired schedule and click **Remove**.

INFO: A schedule cannot be deleted as long as it is still assigned to any queue. Before deleting a schedule, its assignment to the queue(s) must be removed.

18.6.2.8 How to Save a Rule (CCV) as a PDF File

The **Contact Center** wizard enables you to save rules (CCV) as a PDF file. The PDF file can then be typically printed or sent by e-mail.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
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**. The rule will be displayed in the Rule Editor.
7) Click on **Print**. The Save window appears.
8) Enter the name of the file and then select the directory in which the file is to be stored.
9) Click on **Save**.
10) Close the window and confirm the prompt about closing this window with **Yes**.

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.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
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. The rule will be displayed in the Rule Editor.
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.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Download a rule (CCV) in a backup file format.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Schedule**. All existing schedules are displayed.
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. The rule will be displayed in the Rule Editor.
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 How to Add a Queue

Prerequisites

At least one UCD group has been configured.

At least one schedule has been set up.

At least one e-mail account is available for receiving e-mails (if e-mails are to be queued).

The sending of e-mails has been configured in the communication system (if e-mails are to be sent by agents of the queue).

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.

4) Click on **Queue**.
5) Click on **Add**.
6) Click on the **General Settings** tab.
7) Enter the name of the queue in the **Queue Name** field.

   Recommendation: Use the name of one of your configured UCD groups.

   INFO: To ensure that the queue name is displayed fully in a report, you should select short designations and avoid concatenations. Example: Domestic Sales Group 1 (not: DomesticSalesGroup 1)

8) Select one of the following options for the status of the queue:
   - 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.

     The deactivation of a queue leads to the activation of the fallback solution through the associated UCD group. If no agent for the UCD group is logged in, and if no further call forwarding destination has been entered for the UCD group, callers will hear the busy signal.
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.

    If the number of calls waiting in the queue exceeds the number specified here, the queue symbol for the agent changes from green to orange.
13) Enter the alarm threshold value in seconds in the **Queue Alarm Time** field.

    If the waiting time for a queued call specified here is exceeds the time specified here, the corresponding item in the list of Contact Center calls for the agents changes to red.
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.

    Calls abandoned after the specified time has elapsed are included in the statistics.
16) Select one of the following options for the display of screen pops in the myAgent application:

    INFO: Screen pops are needed to accept and execute callbacks and to accept faxes and e-mails.

    - 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) Select one of the following options for the wrapup mode:

For queues with wrapup mode, agents can assign their calls to specific categories (orders, complaints, service, etc.) using wrapup codes.

- 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. The horizontal axis shows the waiting time in the queue, and the vertical axis shows the priority of the selected queue as compared to other queues. 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. This defines the priority of the call types within the selected queue. Higher priorities are assigned by moving the scroll bars incrementally to the right.

INFO: A higher priority should be chosen for voice calls than for other types of calls. Otherwise, waiting callers could be superseded by callbacks, faxes or e-mails.

---

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.

Faxes to these phone number/s will then be added to the queue and treated as incoming calls.

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).

  Select whether e-mails are to be sent via an SSL (Secure Socket Layer) connection. If you want to use an SSL connection, select the **Use SSL connection** check box. (Note that the port number of the E-mail server may be changed as a result. The default port number for POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

  Click on **Save**. 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) Select one of the following options for intelligent call routing within the queue:

- 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**. As a prerequisite, no preferred agent must have been defined for the caller.
- 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) Click on **Save**.

18.6.2.12 How to Edit a Queue

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.

3) Click on **Edit** to start the **Contact Center** wizard.

4) Click on **Queue**.

5) Mark the desired queue and click **Edit**.

6) Click on the **General Settings** tab.

7) Change the desired settings.

8) Select one of the following options for the status of the queue:

- 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.

  The deactivation of a queue leads to the activation of the fallback solution through the associated UCD group. If no agent for the UCD group is logged in, and if no further call forwarding destination has been entered for the UCD group, callers will hear the busy signal.

9) Select one of the following options for the display of screen pops in the myAgent application:

INFO: Screen pops are needed to accept and execute callbacks and to accept faxes and e-mails.

- 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) Select one of the following options for the wrapup mode:

For queues with wrapup mode, agents can assign their calls to specific categories (orders, complaints, service, etc.) using wrapup codes.

- 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. The horizontal axis shows the waiting time in the queue, and the vertical axis shows the priority of the selected queue as compared to other queues. 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. This defines the priority of the call types within the selected queue. Higher priorities are assigned by moving the scroll bars incrementally to the right.

INFO: A higher priority should be chosen for voice calls than for other types of calls. Otherwise, waiting callers could be superseded by callbacks, faxes or e-mails.

---

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).

  Select whether e-mails are to be sent via an SSL (Secure Socket Layer) connection. If you want to use an SSL connection, select the **Use SSL connection** check box. (Note that the port number of the E-mail server may be changed as a result. The default port number for POP3 via SSL = 995). If you do not want to use an SSL connection, clear the **Use SSL connection** check box.

  Click on **Save**. 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) Change the desired settings.
17) Click on **Save**.

18.6.2.13 How to Activate or Deactivate a Queue

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Queue**.
5) Click on **Edit**.
6) Click on the **General Settings** tab.
7) Select one of the following options for the status of the queue:
   - 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.

     The deactivation of a queue leads to the activation of the fallback solution through the associated UCD group. If no agent for the UCD group is logged in, and if no further call forwarding destination has been entered for the UCD group, callers will hear the busy signal.
8) Click on **Save**.

18.6.2.14 How to Configure a Pilot for Incoming Fax Messages in Queues

Prerequisites

At least one fax number for receiving faxes is available.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Click on **Expert Mode** in the navigation bar.
2) In the navigation tree, click on **Telephony Server** > **Stations**.
3) In the menu tree, click on **Stations** > **UC Applications** > **Contact Center Fax**. The logical port numbers intended for fax boxes are displayed.
4) Click on the desired port number in the menu tree.
5) Click the **Edit Station Parameters** tab.
6) Enter the call number of the new pilot for incoming fax messages in the **Call Number** field.
7) Enter the name of the new pilot for incoming fax messages in the **Name** field.

8) Enter the direct inward dialing number of the new pilot for incoming fax messages in the **Direct inward dialing number** field.
9) Click **Apply** followed by **OK**.

The pilot for incoming fax messages can now be activated for the desired queue.

18.6.2.15 How to Define Target Values for the Grade Of Service

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Grade of Service**.
5) Mark the desired queue and click **Edit**.
6) Click on and drag the red dots to the desired positions.

   The horizontal axis shows the waiting time in the queue in intervals of 10 seconds, and the vertical axis shows the target value for the Grade Of Service as percentage values.

   This enables you to specify the target values for quality of switching in the queue. Quality assessments can then be made by comparing these target values with the actual waiting times for callers in the queue.
7) Click on **Save**.

18.6.2.16 How to Define the VIP Caller Priority

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **VIP Caller Priorities**.
5) Mark the desired queue and click **Edit**.
6) Click on and drag the red dots to the desired positions.

   This defines the priority of normal callers as opposed to VIP callers.

   The horizontal axis shows the waiting time in the queue in intervals of 30 seconds, and the vertical axis shows the priority of normal callers who are not registered in the VIP call list directory.

   For example, you can the set the red dots so that a priority of 100 percent is reached after 180 seconds. In this case, normal callers will be treated with

the same priority as VIP callers only after 180 seconds. Earlier incoming calls from VIP callers are given prioritized treatment in the queue.

Alternatively, the values for individual waiting time intervals can also be entered in the input fields on the right next to the graph.

7) Click on **Save**.

18.6.2.17 How to Edit the VIP Call List

Prerequisites

The callers to be placed on the VIP Call List are in the external directory.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **VIP Call List**.
5) Mark the desired queue and click **Edit**.
6) Select one of the following options:
   - If you want to add a caller to the VIP Call List, click **Add** in the upper part of the window. Select the desired entry. Define the priority of this VIP caller as opposed to other VIP callers by dragging the scroll bar to the desired position. Higher priorities are assigned by moving the scroll bars incrementally to the right.
   - If you want to add a call number pattern to the VIP Call List, click **Add** in the lower part of the window. Enter the desired call number pattern (e.g., `089 7577*`) in the Pattern field. Define the priority of all VIP callers with this call number pattern as opposed to other VIP callers by dragging the scroll bar to the desired position. Higher priorities are assigned by moving the scroll bars incrementally to the right.

     It is not possible to enter call number patterns in the canonical call number format. The use of shortcut characters for country codes (for example +49 instead 0049) is likewise not possible. Call number patterns must always be specified without the CO access code.

     Example of a call number pattern: `089 7577*` (089 = area code for Munich, 7577 = PABX number of a company, * = wildcard for any number). By entering this call number pattern in the VIP call list, all callers from Munich, whose telephone number begins with 7577, are given priority.

     The following characters can be used as wildcards (placeholders) in a call number pattern:

     – * = wildcard for any number
     – ? = wildcard for any digit
   - If you want to edit an item in the VIP call list, mark the desired entry and click **Edit**. Change the desired settings.
   - If you want to remove an entry from the VIP call list, mark the desired entry and click **Remove**.
7) Click on **Save**.

18.6.2.18 How to Define Preferred Agents

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
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) Define the priority of the preferred agent if multiple preferred agents were defined. You have the following options:
    - 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 How to Delete Preferred Agents

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Preferred Agents**.
5) Mark the desired queue and click **Edit**.
6) Mark the agent to be deleted in the **Preferred Agents** area.
7) Click on **Remove Agent**.

18.6.2.20 How to Add a Contact Center Break

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Contact Center Breaks**.
5) Click on **Add**.
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) Click on **Save**.
10) If you want to add another Contact Center break, repeat steps 5 through 9.

18.6.2.21 How to Edit a Contact Center Break

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Contact Center Breaks**.
5) Mark the desired Contact Center Break and click **Edit**.
6) Change the required parameters.
7) Select one of the following options:
   - If the Contact Center break should be available to agents, select the **Active** check box.
   - If the Contact Center break should not be available to agents, clear the **Active** check box.
8) Click on **Save**.

18.6.2.22 How to Delete a Contact Center Break

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Contact Center Breaks**.
5) Mark the desired Contact Center Break and click **Remove**.

18.6.2.23 How to Add a Wrapup Reason for a "Simple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Contact Center Wrapup Codes**. All queues for which a wrapup code for "Simple Wrapup" were defined are displayed.
5) Click on **Add**.
6) Select the queue for which you want to add a wrapup reason in the **Queue** drop-down list.
7) Enter a designation for the new wrapup reason in the **Description** field.
8) Click on **Save**.
9) If you want to add another wrapup reason, repeat steps 5 through 8.

18.6.2.24 How to Edit a Wrapup Reason for a "Simple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Contact Center Wrapup Codes**. All queues for which a wrapup code for "Simple Wrapup" were defined are displayed.
5) Mark the desired entry and click **Edit**.
6) If you want to assign the wrapup reason to another queue, select the new queue in the **Queue** drop-down list.
7) If you want to change the designation of the wrapup reason, enter the new designation in the **Description** field.
8) Click on **Save**.

18.6.2.25 How to Delete a Wrapup Reason for a "Simple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.

4) Click on **Contact Center Wrapup Codes**. All queues for which a wrapup code for "Simple Wrapup" were defined are displayed.
5) Mark the desired entry and click **Remove**.

18.6.2.26 How to Add a Wrapup Reason for a "Multiple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Multi-Wrapup Code**.
5) Select the desired queue in the **Contact Center Queue** drop-down list. The groups and subgroups already defined for this queue are displayed.

NOTICE: Below each group or subgroup (if any), at least one item should also be configured, to be able for the agent to wrapup a call. Wrapping a call up is not possible if a group or subgroup is empty.

---

6) If you want to combine the new wrapup reason in a group with other wrapup reason, select one of the following options:
   - If you want to assign the new wrapup reason to an existing group or subgroup, select the desired group or subgroup and click **Add Item**. Enter a designation for the new wrapup reason in the **New Wrapup Item** field and click **OK**.
   - If you want to assign the new wrapup reason to a new group, click **Add Group**. Enter a designation for the new group in the **Group Name** field and click **OK**.

     Select the new group and click **Add Item**. Enter a designation for the new wrapup reason in the **New Wrapup Item** field and click **OK**.
   - If you want to assign the new wrapup reason to a new subgroup, select the desired group and click **Add Group**. Enter a designation for the new subgroup in the **Group Name** field and click **OK**.

     Select the new subgroup and click **Add Item**. Enter a designation for the new wrapup reason in the **New Wrapup Item** field and click **OK**.
7) If you want to add another wrapup reason, repeat steps 5 and 6.

18.6.2.27 How to Edit a Wrapup Reason for a "Multiple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Multi-Wrapup Code**.
5) Select the desired queue in the **Contact Center Queue** drop-down list. The groups and subgroups already defined for this queue are displayed.
6) Mark the group or subgroup to which the wrapup reason to be edited is assigned. All wrapup reasons (items) assigned to this group will be displayed.
7) Mark the wrapup reason to be edited and click on **Rename Item**.
8) Enter a new designation for the wrapup reason in the **Rename Wrapup Code** field and click **OK**.
9) If you want to change the designation of the group or subgroup, click on **Rename Group**.
10) Enter a new designation for the group or subgroup in the **Group Name** field and click **OK**.

18.6.2.28 How to Delete a Wrapup Reason for a "Multiple Wrapup"

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Multi-Wrapup Code**.
5) Select the desired queue in the **Contact Center Queue** drop-down list. The groups and subgroups already defined for this queue are displayed.
6) Mark the group or subgroup to which the wrapup reason to be deleted is assigned. All wrapup reasons (items) assigned to this group will be displayed.
7) Mark the wrapup reason to be deleted and click on **Remove Item**.
8) If you want to delete the group or subgroup, click on **Remove Group**.

18.6.2.29 How to Assign an Agent to a Queue

You can assign agents to one or more queues with the **Contact Center** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Queue Bindings**. All existing queues will be displayed.

5) Select the queue to which you want to assign an agent and click on **Edit**. All agents already assigned are displayed.
6) Click on **Add** to add the appropriate agent into the desired queue. The **Add** window is then displayed.
7) Select one of the following options:
   - If the agent is to receive calls without regard to the load on the queue, select **Primary Agent** from the **Type** drop-down list.
   - If the agent is to receive calls only when the queue overflows, select **Overflow Agent** from the **Type** drop-down list..
8) If you have selected **Overflow Agent**:
   a) Enter the time after which incoming calls for an agent should be forwarded in an overflow situation in the **Overflow after seconds in queue** field.
   b) Enter the maximum number of calls in the **Overflow after calls in queue** field. Calls that exceed this maximum number are received by an overflow agent.
9) Enter a percentage value for the **Skill Level** of the agent.

   Skill levels enable you to control the distribution of calls to agents in a queue. Agents with higher skill levels are given preference during the call distribution. In cases where all agents have the same skill level, the longest idle agent receives the call.
10) Select one of the following options:
   - If the agent is to receive callback requests in the form of voice messages, select the check box **Enable agent callback**.
   - If the agent is to be prevented from receiving callback requests, clear the **Enable agent callback** check box.
11) Enter the automatic work time in seconds for the agent of this queue in the **Work Time** field.
12) Click on **Save**.
13) If you want to assign further agents to the queues, repeat steps 5 through 12.

18.6.2.30 How to Remove an Agent from the Queue

You can remove agents from one or more queues with the **Contact Center** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **Contact Center** wizard.
4) Click on **Queue Bindings**. All existing queues will be displayed.
5) Select the queue from which you want to remove an agent and click on **Edit**. All agents already assigned are displayed.
6) Select the desired agent and click on **Remove**.

7) If you want to remove further agents from queues, repeat steps 5 and 6.

18.7 Notes on Using the Contact Center

This section contains information about some special aspects and possible restrictions to be observed when using the Contact Center.

18.7.1 Restrictions on Operating the Contact Center

The operation of the Contact Center is subject to certain conditions. In addition, there are some restrictions on the use of system features by agents.

Conditions for the Operation of the Contact Center

The following conditions for the operation of the Contact Center must be taken into account:

- Trunks

  The Contact Center does not support analog trunks (MSI). All external connections of the Contact Center must be made via ISDN or IP telephony. It should be noted that the integration of IP telephony is only possible through certified Internet Telephony Service Providers (ITSPs).
- Networking

  In a networked scenario, all agents must be connected to the communication system in which the Contact Center is configured.
- Agent telephones

  Agents can use all system telephones (IP phones (HFA) such as OpenStage 40, for example, or $U_{P0/E}$ phones such as OpenStage 40 T) and DECT telephones. Note that only the DECT telephones that are currently released for operation with OpenScape Business Cordless may be used.

  It is not possible to use analog, ISDN and SIP telephones here.

  Agents are not allowed to be members of a group (Group Call, Hunt Group) or a MULAP. This restriction also applies to system features used in combination with MULAPs, i.e., Team Configuration (Team Group), Executive/Secretary (Top Group) and Mobility Entry.
- myAgent

  myAgent should not be used simultaneously with other UC clients, since mutual interference with the presence status cannot be excluded (see Notes on Using myAgent and UC Suite Clients Simultaneously). During normal operation of the Contact Center, agents use only myAgent to change their status (logged in, logged out, available, etc.).

- Connecting applications via the CSTA interface

  It is possible to connect applications via the CSTA interface, provided the following conditions are met:

  – The application should not produce any significant additional load on the CSTA interface.

    Consequently, the connection of unified communications or call distribution solutions, CTI power dialers or even CTI solutions with many intensively used individual CTI clients is not allowed.
  – The application must not control any agent telephones via the CSTA interface or set up any call forwarding for the agent telephones.

    Consequently, the connection of CTI applications for agents, rule assistants or personal assistants is not allowed.

  The connection of TAPI 120/170 has been basically approved. For the load of the communication system, the same conditions as for the connection of other applications via the CSTA interface apply. In connection with the Contact Center, TAPI 120/170 should preferably be used to connect CRM (Customer Relationship Management) or ERP (Enterprise Resource Planning) systems, provided they support TAPI.

Restrictions on Using System Features

The following system features are not available to agents or are subject to restrictions. These features are, however, not mandatory for agents, since the allocation of calls is handled automatically by the Contact Center. The allocation depends on the set rules and the availability of agents.

- Locked Features

  The activation of system features via myAgent and the associated agent telephone is not supported for the available agents of the Contact Center. Agents can activate system features only via myAgent.

  The following system features are therefore not supported in conjunction with myAgent:

  – Call waiting
  – Second call
  – Parking
  – Group Call
  – Do Not Disturb (for logged in agents)
  – Intrusion on an agent call (exception: agents with the authorization level of a Supervisor or Administrator)
  – Features that affect call routing and active call connections

- Features that affect call routing

  The following features could potentially change the call routing in the contact center and should therefore not be executed by agents.

  – Call forwarding

    If a logged in agent activates call forwarding, a logout occurs.

    Call forwarding is disabled as soon as an agent logs into a queue.
  – Do Not Disturb

    If a logged in agent activates Do Not Disturb via a UC client, an automatic logout occurs.

    Do not Disturb is disabled as soon as an agent logs into a queue.
  – Relocate

    Relocating a telephone changes the logical assignment of the station numbers. The new station number assignment is only transmitted after restarting the Contact Center.
  – Night service

    When setting up a night service in the communication system, it must be ensured that the configurations of the Contact Center-related parameters (agents, queues, etc.) for the day and night service are identical.
- Features that affect reports

  Executing the following features from an agent telephone can lead to a distortion of the information in reports:

  – Call pickup of Contact Center calls by non-agents
  – Call transfers (e.g., via the Direct Station Select (DSS) key) of Contact Center calls to non-agents
  – Conferencing
  – Toggle/Connect
  – Parking

  INFO: The "Consultation Hold" feature is transparent for the presentation of Contact Center calls in reports and can be used by agents, regardless of the consultation destination.
- Roles and functions not relevant for agents

  The following functions are not relevant, since the "Call Waiting" feature (also called "camp on") is blocked for agents.

  – Attendant Console
  – Hotline destination

18.8 Notes on the Use of DECT Phones

DECT telephones can be used as phones for contact center agents. However, the differences in the operating procedure as compared to corded phones must be taken into account.

Prerequisites for the Use of DECT Phones

- Only the DECT telephones that are currently released for operation with HiPath Cordless Office and OpenScape Business Cordless may be used.
- The area within which the contact center agents move about must provide a complete wireless coverage.
- The number of base stations must be such that enough B-channels are available for the DECT telephones of the contact center agents.
- As far as possible, a contact center agent should not leave the wireless range while logged into a queue of the contact center.

Differences in the Operating Procedure as Compared to Corded Phones

- Logging into a queue of the contact center is only possible through myAgent.
- No messages such as **Available** or **Break**, for example, appear in the display of the DECT telephone.
- The control of a DECT telephone via myAgent (e.g., via the **Telephony** area of the myAgent main window or the screen pop of the incoming myAgent call) is not possible.
- Incoming calls can only be accepted via the DECT telephone.
- Outbound calls must be initiated via the DECT telephone.

Aspects to be considered when using DECT phones:

- Search time

  For an incoming call, the time required to find the DECT telephone may take several seconds (at worst up to 20 seconds) before a call is signaled on the DECT telephone. During the search time, the caller hears the ringing tone.

  The contact center evaluates this time as "pickup time". The actual pickup time by a contact center agent thus consists of the search time and the alert time (i.e., time until the call is answered).

  If a contact center agent leaves the wireless range with his or her DECT telephone, this may result in longer search times.
- DECT telephone cannot be found

  If a contact center call exceeds the prescribed time for a call to be answered by the agent (e.g., because the contact center agent is out of range), the agent is automatically logged out of the queue or queues involved. Logging in again is only possible through myAgent.

18.9 Reports

Reports are used to determine the current status of the Contact Center and to analyze the strengths and weaknesses of its associated components. This makes it possible to optimize the Contact Center configuration, for example, and to thus use the Contact Center resources more efficiently. The Contact Center provides users with real-time reports as well as historical reports.

Real-time Reports

Real-time reports are continuously updated. They provide important information such as details on agent utilization, the grade of service, abandon rates and average processing times. Using these continually updated and filterable caller lists, the progress of a customer contact can be examined in stages. In addition, the activities of all agents can be reviewed. This information can be used for training purposes, for example, and for contact analysis and wrap-up activities.

Agents with the authorization level of a Supervisor or Administrator can be acoustically and visually informed when definable operating parameters are exceeded. Appropriate thresholds for each queue can be defined individually.

Historical Reports

By selecting data elements and user-specific report parameters, historical reports can be set up quickly and retrieved in graphic or tabular form.

Using the myAgent application, more than 20 predefined report templates can be used for standard reports.

The optionally available myReports application expands the options for creating historical reports with over 100 predefined report templates. The report generation can be individually scheduled, and the prepared reports can be automatically sent at scheduled times in standard export formats to predefined e-mail addresses or stored at a location configured by the myReports administrator.

INFO: Reports based on the call history stored in the communication system. The maximum retention period for the call history is 365 days (default setting). An administrator with the **Expert** profile can set the retention period for the call history on a system-wide basis.

Example: The retention period was set to 100 days. This means that only data that is up to 100 days old can be used for the preparation of reports.

Data Protection

If the myReports administrator enabled data protection when configuring myReports, the last four digits of the phone numbers (CLI column) will be replaced by **** in all relevant reports.

If the subscriber has flagged his or her private number, mobile number, external number 1 and/or external number 2 as invisible, these phone numbers will not be displayed in all relevant reports.

18.9.1 Predefined Report Templates

myReports provides more than 100 predefined report templates for creating reports.

These templates are classified by subject area and assigned to the following report groups:

- **Agent Activity**
- **Agents**
- **CLI**
- **Call History**
- **Calls**
- **Fax / E-Mail**
- **Other**
- **Performance**
- **Queues**

- **User Presence Status**
- **Wrap-up Codes**

19 Mobility

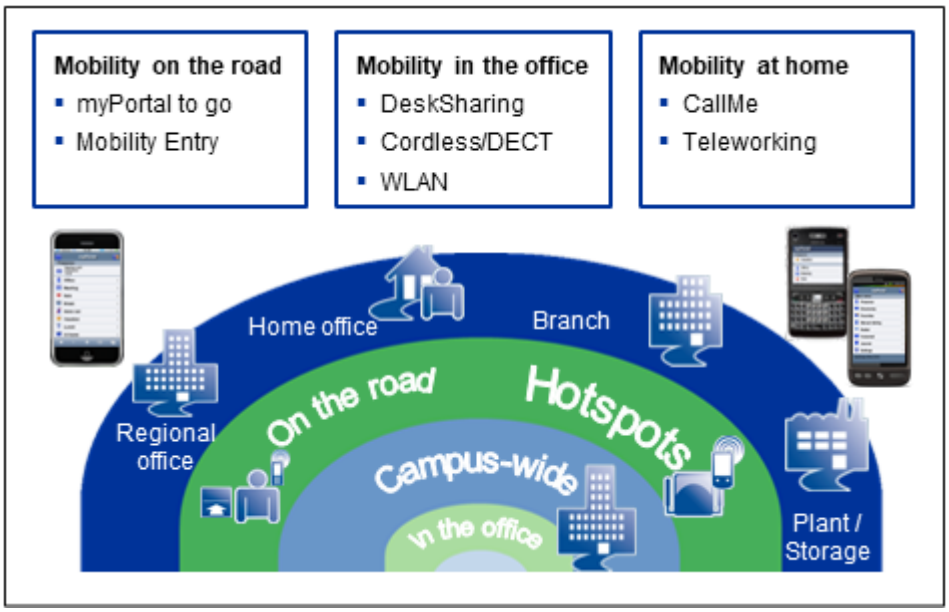
OpenScape Business provides integrated mobility solutions for any business. This typically includes the integration of mobile phones/smartphones, the usage of Cordless/DECT and WLAN phones, etc., down to Desk Sharing and teleworking. Mobility includes Mobility on the road, Mobility in the office and Mobility at home.

Related concepts

Stations on page 406

19.1 Integrated Mobility Solution

The mobility solutions integrated in the communication system provide efficient communication everywhere and with a wide variety of endpoints.



19.2 Mobility on the Road

Mobility on the road is achieved through the integration of mobile phones via myPortal to go or Mobility Entry. The One Number Service enables a subscriber to be reached through a single phone number worldwide. Furthermore, with dual-mode telephony, additional cost savings can be achieved if the subscriber is within range of a WLAN.

Mobility on the road is the combination of:

- Office phone and smartphone (myPortal to go)
  - Availability under one number (One Number Service)
  - Control of features via the web client
  - UC features such as control of the presence status

- Office phone and mobile phone (Mobility Entry)
  - Availability under one number (One Number Service)
  - Control of features via DTMF codes

In addition to the combination of mobile phone and office phone, it is also possible to configure a mobile phone alone (i.e., without a parallel office phone) to be reached under a land-line number.

Full functionality is achieved with system telephones (HFA). SIP phones can be used with restrictions.

19.2.1 myPortal to go

myPortal to go is a powerful unified communications application for smartphones and tablet PCs which provides access to the unified communications features of the communication system. Besides convenient dialing aids via phone directories and favorites, and information on the presence status of colleagues, it can, for example, also be used to access voicemails.

myPortal to go is available in three variants:

- 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)
- as a Web Edition for mobile web browsers with HTML5 support, e.g., for the Windows Phone (version 8.0 or higher) or BlackBerry (version 10 or higher) operating systems:

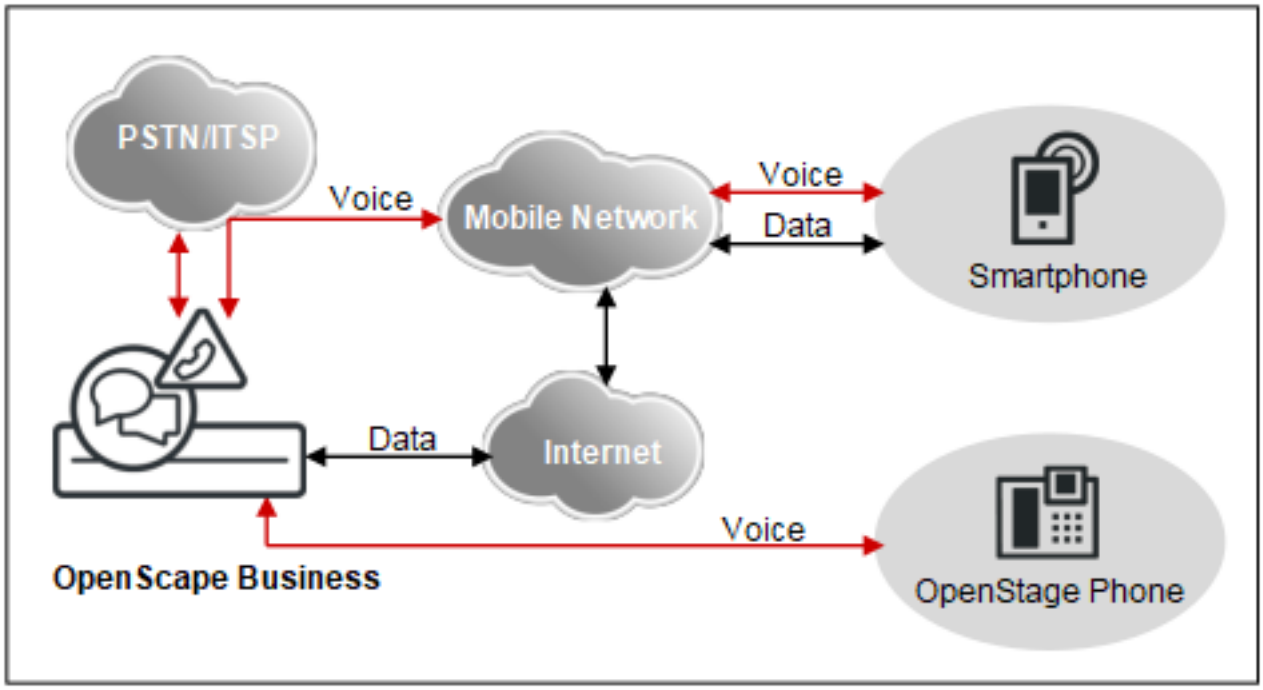
  `http://<IP address of the communication system>:8801`

  `https://<IP address of the communication system>:8802`

  For security reasons it is recommended that only https be used. This requires port forwarding to be set up in the router from external TCP/443 to internal TCP/8802.

  NOTICE: Please note that by using myPortal to go Web Edition with Desk phone operating mode, telephony is not possible from the client. You can place calls but payload will go through the desk phone which is connected.

myPortal to go can be used both on pure GSM mobile phones as well as dual-mode phones. In order to use myPortal to go, a mobile phone contract with data option (flat rate recommended) is required.



Apart from a few exceptions (e.g., access to contact details in the mobile phone), the scope of features is identical in all variants.

myPortal to go supports the following features:

- Presence status
- Status-based call forwarding
- CallMe service (only with UC Suite)
- Directories
- Favorites List
- Journal
- Search by phone number and name
- Call Functions
- One Number Service (ONS)
- Voicemail
- Text messages

CTI Features During a Call:

- Consultation
- Toggle/Connect
- Attendant
- Conferencing
- Disconnect

myPortal to go can be used with both the UC solutions, UC Smart and UC Suite. Depending on the UC solution and the licenses assigned to you, the scope of the available features may vary slightly.

myPortal to go supports the following operating modes:

- Mobility:

  Unrestricted access to the telephony and UC features, regardless of location (including One Number Service).

- Desk phone:

  Use of UC features and as a convenient dialing aid for the office phone (without One Number Service).

Other features can be used with the UC clients (e.g., myPortal for Desktop)

myPortal to go establishes an encrypted connection (https) to the OpenScape Business UC Server. If the connection is interrupted (offline mode), you can still select and dial cached entries from the journal and the favorites list via GSM and perform GSM dialing manually.

NOTICE: For supporting mobility, myPortal to go has to be firstly registered as VoIP (HFA) user so that the Openscape Business System side relevant port to become active.

Dialing mode of myPortal to go

Smartphone users can choose between different dialing modes for outbound calls, depending on which operating mode is set as the intended use.

- Call through (only in the Mobility mode)
- Preferred callback (only in the Mobility mode)
- Associated dialing (only in the Mobility mode)

  myPortal to go controls the connection setup for the desk phone at the workplace. If a SIP phone or a SIP softclient is controlled via associated dialing, some CTI features such as consultation holds and conferencing are not available.

19.2.1.1 Prerequisites for myPortal to go

In order to use myPortal to go, the smartphone must be equipped with the appropriate hardware and software.

The following requirements apply:

- myPortal to go as Mobile UC App: Android operating system (version 5.0 or higher) or Apple iOS (version 12.5 or higher)
- myPortal to go as Web Edition: Mobile web browser with HTML5 support, e.g., for the Windows Phone (version 8.1 or higher) or BlackBerry (version 10 or higher) operating systems. Web browsers without TLS 1.2 support are not supported anymore.

  To enable access, port forwarding must be set up in the router from external TCP/443 to internal TCP/8802 (https) or internal TCP/8801 (http). For security reasons it is recommended that only https be used.
- myPortal to go iOS client:
  - A proper DNS server needs to be configured and internet access has to be granted so that public domain names can be resolved, and push notification messages can be send to the iOS device via Apple's APNS servers.
  - If the company firewall restricts outbound internet access, make sure that the firewall is open for APNS on port TCP/443.
  - For iOS push notifications, it is mandatory to keep the system software up to date, because mandatory certificates for communication with

Apple's APNS service will be updated frequently with major/minor system releases and fix releases.

– Latest versions of myPortal to go (iOS) support Apple's CallKit API. CallKit is a framework that aims to enhance the VoIP experience by allowing myPortal to go (iOS) to integrate with the native device calling features. The minimum required system software version is V3R2.

  Current myPortal to go (iOS) clients will not be able to login to older OpenScape Business versions.

– iOS security requirements apply when connecting to the communication server. The current Openscape Business auto-generated self-signed certificate is not sufficient if the app connects to the communication server using a domain name instead of a server IP address. Apple has revised its security requirements for TLS server certificates https://support.apple.com/en-us/HT210176.

  To avoid problems when myPortal to go (iOS) cannot establish a connection to the communication server, we recommend either connecting to the communication server via the IP address or installing a trustworthy SSL certificate on the server side.

- Touch screen (recommended for ease of use)
- Display resolution for smartphones: at least 240 pixels * 320 pixels (recommended: 320 pixels * 480 pixels or higher)
- Display resolution for tablet PCs: at least 800 pixels * 480 pixels (recommended: 1024 pixels * 600 pixels or higher)
- Internet access
- Support for the simultaneous transmission of voice and data through mobile phones and the mobile network
- A stable 3G/4G/5G data connection. Please note that slow connections - in particular 2G/EDGE/GPRS - can lead to poor user experience and functional limitations (VoIP).

  Alternatively: a pure WLAN connection with a SIP client for telephony.
- Flat rate data plan is strongly recommended..

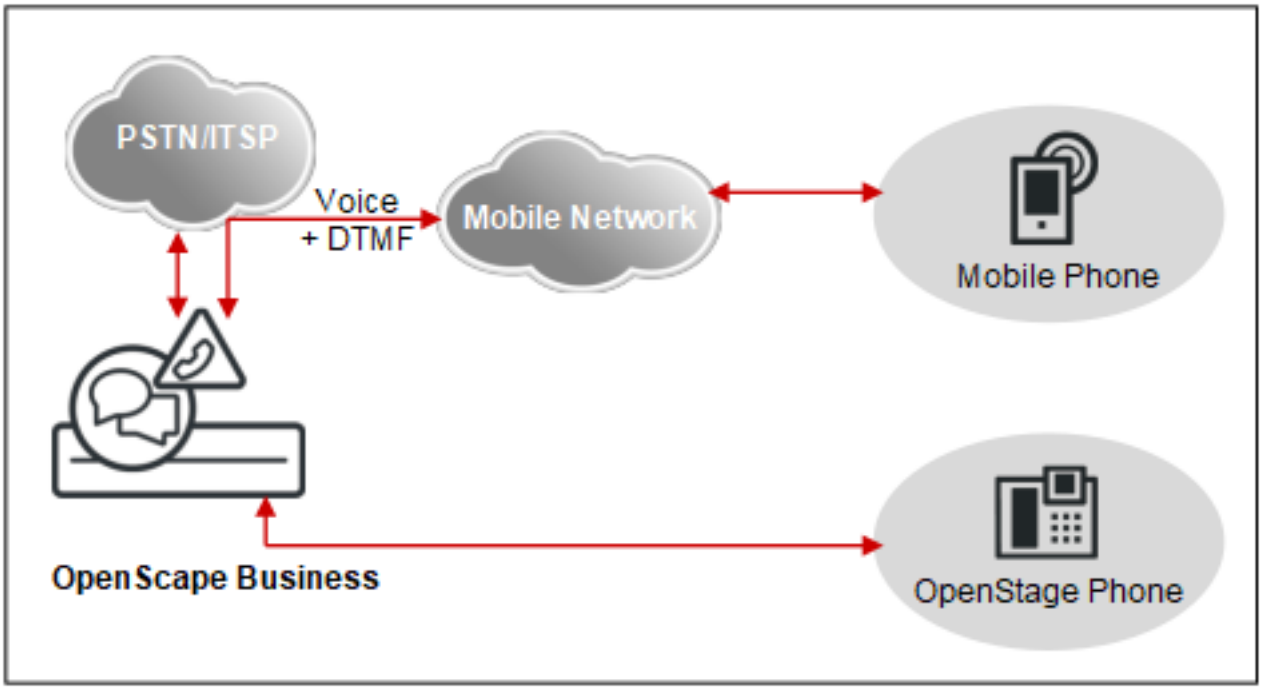
The mobile UC app can be downloaded free of charge from the Google Play Store or the Apple App Store.

Depending on which device and operating system is used, the ease of use or function may be affected. Support is only provided if a reported problem with a reference device can be reproduced. For more information on reference devices, browsers and operating systems, refer to the Release Notes and the Experts wiki at `https://wiki.unify.com/wiki/myPortal_to_go`.

19.2.2 Mobility Entry

Mobility Entry enables the integration of mobile phones. This provides subscribers with access to certain system features via mobile phones.

Mobility Entry enables subscribers to control voice connections using DTMF after dialing into the system.



Dialing Methods for Mobility Entry

Mobile phone users can choose between different dialing methods for outbound calls.

Mobility Entry offers the following dialing methods:

- Callback
- Call Through

If a mobile phone subscriber at the communication system calls a special DID number with a callback, the call is automatically terminated before the connection is established, and a callback is executed immediately. After the callback, no further authorization is necessary. The mobile phone subscriber can conduct internal and external calls and also use all Mobility features via the communications system.

The prerequisites for a callback are as follows:

- The external number of the calling telephone must be registered and configured at the communication system. If not, the call is disconnected, and no callback is executed.
- The DISA direct inward dialing number has been configured.
- The external number of the mobile phone subscriber is transmitted to the communication system (CLIP information).

Features in a Dormant State

- Dial a number
- Program or delete call forwarding
- Activate or deactivate Do Not Disturb
- Send message
- Reset all services
- Activate or deactivate station number suppression (CLIR)

Features in the Call State

- Consultation
- Alternate (Toggle/Connect)
- Conferencing
- Disconnect and return to held call
- Activate callback
- Enabling DTMF suffix dialing

The signaling of features is handled via system codes (e.g., *1 to program call forwarding).

NOTICE: For Mobility Entry users, the station flag **Disa Class of service** must be enabled.

A maximum of 16 DTMF code receiver resources are available with OpenScape Business X, i.e., a maximum of 16 subscribers (analog, Mobility, etc.) can simultaneously reserve DTMF code receivers. Subscribers for whom the **DTMF-based feature activation** flag is set reserve one code receiver each for the duration of the call.

With OpenScape Business S, the control of features using DTMF codes is supported if the DTMF digits are transmitted as per RFC 2833. If an external Session Border Controller (SBC) is used in the network, no DTMF detection is possible.

NOTICE: Mobility entry must be only configured at nodes with direct CO access.

Related concepts

One Number Service (ONS) on page 907
Comparison between Mobile Clients and Mobility Entry on page 904
Dependencies for Mobile Clients and Mobility Entry on page 906

19.2.3 Comparison between Mobile Clients and Mobility Entry

The mobile clients myPortal Mobile, myPortal to go and Mobility Entry support different features.

Feature	**myPortal to go**	Mobility Entry
General functions		
Mobile phone contract with data option	Yes (flat rate recommended)	no
Parallel call signaling on system telephone and mobile phone (twinning)	yes	yes
Transfer of caller number to the mobile phone (if the network transmits external phone numbers as CLIP; CLIP no screening)	yes	yes

Feature	**myPortal to go**	Mobility Entry
One Number Service (if the network transmits external numbers as CLIP, CLIP no Screening))	yes	yes
Do not Disturb / Disablable call forwarding	no	yes
Station number suppression, enablable/disablable	no	yes
Automatic identification of registered stations	yes	yes
Operation without the Office phone (as a virtual station)	yes	yes
Can be used with OpenScape Business S	yes	yes
Presence status, Journal, voicemail box		
Change own presence status	yes	no
View presence status of other subscribers	yes	no
Journal	New, All, Missed, Answered, Inbound, Voicemail	no
Shared voicemail box; can also be checked on the go	yes	yes
Display received voicemail	Display new, retrieved and saved voicemails	no
Dial		
Access to contacts in mobile phone	yes	yes
Access to contacts in the communication system	External directory (UC Suite), internal directory, personal contacts and system directory	no
Favorites	yes	no
Manual dialing	yes	yes
Redialing	yes	no
Dialing method	Callback, Call Through, Associated Dialing	Callback, Call Through
During the call		
Consultation	yes (not with SIP phone)	yes
Alternate (Toggle/Connect)	yes (not with SIP phone)	yes
Attendant	yes (not with SIP phone)	yes

Feature	myPortal to go	Mobility Entry
Conferencing	yes (not with SIP phone)	yes
Callback on free and busy	no	yes
Call pickup from mobile phone to system telephone	yes	yes
Busy indicator also for calls at the mobile phone (with One Number Service)	yes	yes

Related concepts

Mobility Entry on page 902

19.2.4 Dependencies for Mobile Clients and Mobility Entry

myPortal to go and Mobility Entry have dependencies on other features (e.g., DISA).

Dependency	myPortal to go	Mobility Entry
Mobility Callback DID	For the Mobile Callback dialing mode, the Mobility Callback DID must be configured.	
External destination phone number	Dialing external destination phone numbers by the mobile subscriber is controlled by the system because of the LCR configuration. Dialing can therefore be performed via the ISDN fixed network, analog fixed network or via ITSP.	
Activate CLIP No Screening	You cannot display a caller's number on the mobile station unless it was supplied unverified by the network provider.	
Mobile subscriber CLIP	The CLIP of the mobile subscriber must be transmitted to the communication system. This must be made available by the network provider.	
LCR Administration	As some network providers (fixed-network or ITSP) do not accept destination numbers with a separate international prefix, the system must delete this prefix from these destination numbers. This can be performed in least cost routing (LCR).	
B channels / External connections	The number of B channels depends on the connection duration or the number of mobile stations. Every incoming external call to a mobile subscriber requires two voice channels in the system. If there are not enough voice channels available, it may not be possible to reach a mobile subscriber, and the mobile subscriber may not be able to initiate any calls with the One Number Service.	
Emergency Numbers	When a mobile user dials an emergency number via the communication system, the location of his or her mobile phone cannot be identified. It is therefore advisable to dial an emergency number directly.	
Dialing internal station numbers	When dialing internal phone numbers in international format (e.g., 0004989100) at the mobile station, the location number of the communication system must be configured. Otherwise, internal destinations are routed via the exchange, which can result in costs.	

Dependency	myPortal to go	Mobility Entry
Directory maintenance	To ensure that the called party can be reached when dialing from directories in all dialing modes, all external phone numbers should be entered in canonical format (e.g., +49 89 100).	-
Firewall	A data channel is set up to the integrated web server of the communication system. Consequently, port forwarding to port 8801 (http) and port 8802 (https) must be configured in the firewall. However, it is recommended not to configure any port forwarding for port 8803 (https) in order to access UC Smart Assistant.	-
Data connection	It is advisable to sign a mobile phone contract with a flat-rate data plan. Users of volume rates should disable the "Auto Refresh" option in the settings of myPortal to go.	-
Parallel connections	For some features, a simultaneous voice and data connection is required. This must be supported by both the mobile network providers and the mobile devices.	-
Connection setup from the communication system to mobile stations via	All feature types	All line types that support DTMF transmission.

Related concepts

Mobility Entry on page 902

19.2.5 One Number Service (ONS)

The One Number Service (ONS) effectively makes mobile phones operate as fixed network extensions. This means that subscribers can be reached under one phone number world-wide and can identify themselves only by their respective fixed network numbers.

Setting up a team configuration enables the One Number Service with a single phone number for the workplace (system telephone) and the mobile phone. The caller dials the system phone's number (fixed network). Outgoing calls from mobile phones are signaled to the called party with the fixed network number. Another advantage of the One Number Service is the busy indicator for the mobile subscriber.

Related concepts

Mobility Entry on page 902

19.2.6 Dual-Mode Telephony

Dual-mode mobile phones support both GSM/UMTS networks and WLAN networks. Registration at the communication system is possible over a WLAN either as SIP station or as system client (i.e. HFA station).

If the dual-mode mobile phone is in the WLAN range, it is automatically called as system client (HFA station) or SIP station. If it is outside the WLAN range, the dual-mode mobile phone is called via GSM/UMTS (i.e., mobile phone integration functionality is available).

NOTICE: Dual mode for HFA is supported only when using myPortal to go client and not with other devices or clients.

Automatic forwarding to the GSM phone number only works if the associated HFA or SIP station is entered in the system as a mobile phone station (mobile phone integration). This means that if the HFA or SIP station is registered, it is called as HFA or SIP station, and if it is not registered, it is called via the GSM phone number assigned in the mobile phone integration configuration. CTI call features are not available for SIP clients in myPortal to go. Call control usually occurs within the HFA or SIP clients instead (see also the Release Notice and `http://wiki.unify.com`).

Calls on the company premises occur over the WLAN. As long as calls are made over the WLAN, no call charges are incurred on the mobile phone. Handover and roaming are supported within the WLAN range (if the wireless LAN infrastructure is designed for it), but not from WLAN to GSM, and vice versa.

19.2.7 Configuring myPortal to go and Mobility Entry

myPortal to go (Web Edition) and Mobility Entry are configured with the **Mobile Phone Integration** wizard.

Using the **Mobile Phone Integration** wizard, the administrator can:

- Set up the One Number Service
- Set up myPortal to go (Web Edition)
- Set up Mobility Entry
- Set up dual-mode phones

The mobile phone integration of GSM phones occurs via virtual stations. Features are transferred to the mobile station in this way. Every station with a corresponding license (mobility user) can be assigned a maximum of one mobile station

Operating Modes of Mobile Phones

The following operating modes are implemented for mobile phones:

- **GSM Mode**

  Calls to the internal mobile call number are signaled at the GSM mobile phone.

- **WLAN Mode**

  If the WLAN mobile phone is reachable via the WLAN, the call is conducted via the WLAN. If the WLAN is not available, the call is made via GSM.

Twinning

Calls are signaled in parallel at the mobile phone and the system telephone (twinning). To implement twinning, a team configuration must be set up once the configuration of the **Mobile Phone Integration** has been completed. To do this, use the **Team Configuration** wizard and first select the phone number under which the parallel signaling is to occur (e.g., the system telephone). For the use of myPortal to go (Web Edition), the last step is to reconfigure the user name to the team group in the **Mobile Phone Integration** wizard. On the system telephone, a Direct Station Select (DSS) key to the Mobility stations can be programmed for the seamless (i.e., uninterrupted) transfer of mobile phone calls. Full functionality is achieved with system telephones (HFA). SIP phones can be used but are subject to certain restrictions, e.g., they do not support MULAP keys.

Related concepts

Configuring Team Configurations / Team Groups and Executive/Secretary Functions / Top Groups using Wizards on page 680

Prerequisites for Application Launcher on page 1133

19.2.7.1 How to Integrate GSM Mobile Phones

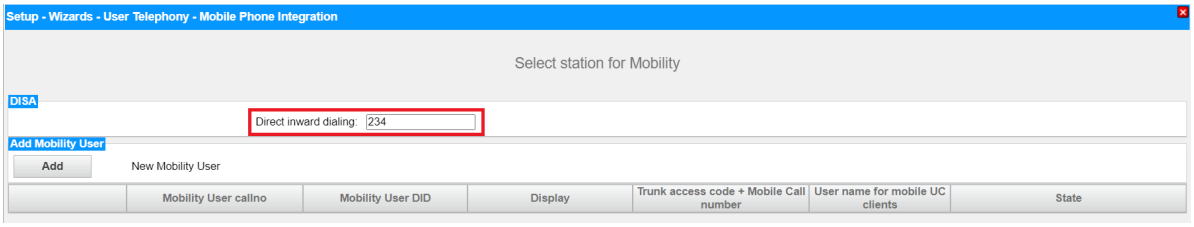
Mobile phones can be integrated in the communication system with the **Mobile Phone Integration** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Mobile Phone Integration** wizard. The **Select Station for Mobility** window appears.
4) Under **DISA access**, select (or enter) the **DID** number with which mobile stations can dial into the communication system.



NOTICE: DISA is required for Mobility Entry (to control the system using DTMF) and for myPortal for Mobile (only when using Call Through).

5) Click on **Add** or **Edit** for the appropriate subscriber whose GSM mobile phone is to be integrated into the communication system. The **Assign Mobility Stations** window appears.

6) Select **GSM Mode** as the mode for your mobile phone operation.

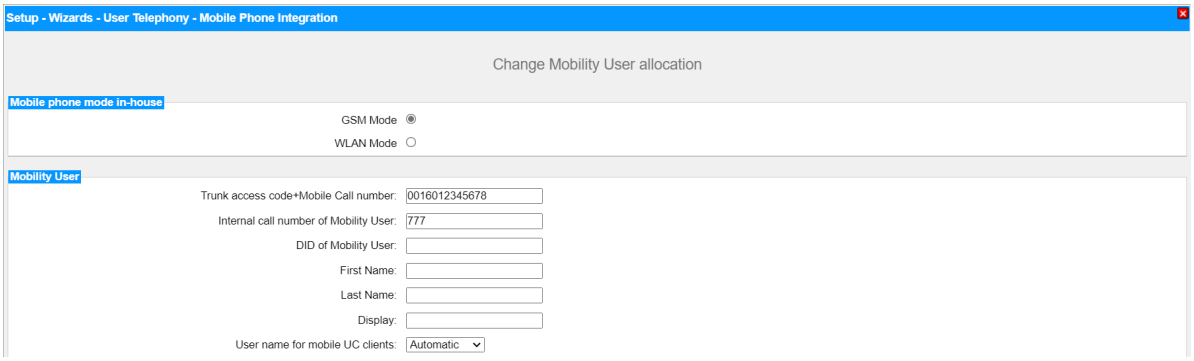
7) Under **Trunk access code+Mobile phone number**, enter the phone number of the mobile phone (e.g., 0016012345678).

8) Under **Internal call number of the Mobility station**, enter the corresponding internal number (e.g., 777) an **internal name** and the **DID number** of your choice. Note that the internal call number must not have been already assigned.

INFO: If you want to use DID 879, 890 or 891, you must make the setting through ManagerE and not through WBM.

---

9) In the **Username for myPortal to go (Web Edition)** drop-down list, select **Automatic**; this will cause the internal number of the user to be used as the user name.



10) Only with UC Smart: Assign a mailbox to the station if needed:

a) Select whether the station is to receive a default mailbox or an attendant mailbox (AutoAttendant) in the **UC Smart Mailbox type** drop-down list.

b) Only with default mailbox: If a caller may leave a message in the voicemail box, select the **Recording** check box.

c) Select a greeting from the **Greeting** drop-down list.

d) If the password of the voicemail box is to be reset, select the **Password Reset** check box.

NOTICE: The **Password Reset** check box must be cleared when setting up a new voicemail box. It is used to reset the password of the voicemail box. When a new voicemail box is created, the subscriber must change the initial password anyway when accessing his or her voicemail box for the first time.

---

11) Click **OK & Next**.

12) Click **OK & Next** followed by **Finish**.

19.2.7.2 How to Integrate Dual-Mode Telephones (GSM/WLAN) with HFA or SIP Client

The **Mobile Phone Integration** wizard can be used to configure a mobile phone as a dual-mode phone with system client (HFA client) or SIP client (WLAN mode).

Prerequisites

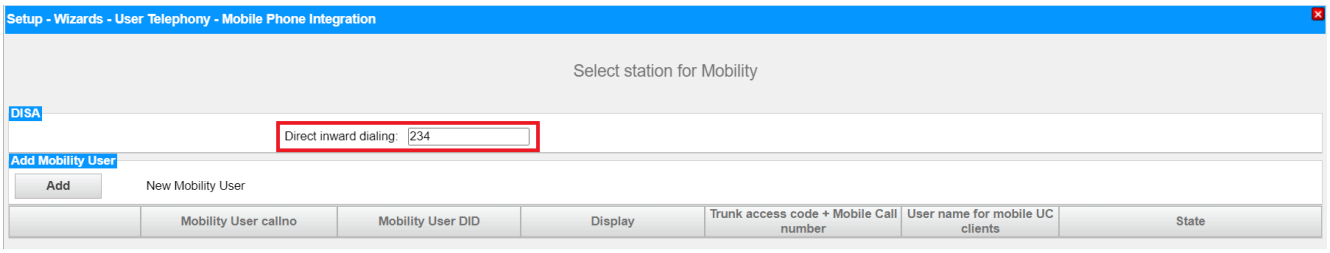
You are logged on to the WBM with the **Advanced** profile.

The HFA device or SIP station must be configured via the WBM.

Mobility user license has been assigned to the subscriber.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click **Edit** to start the **Mobile Phone Integration** wizard. The **Select Station for Mobility** window appears.
4) Under **DISA access**, select (or enter) the **DID** number with which mobile stations can dial into the communication system.

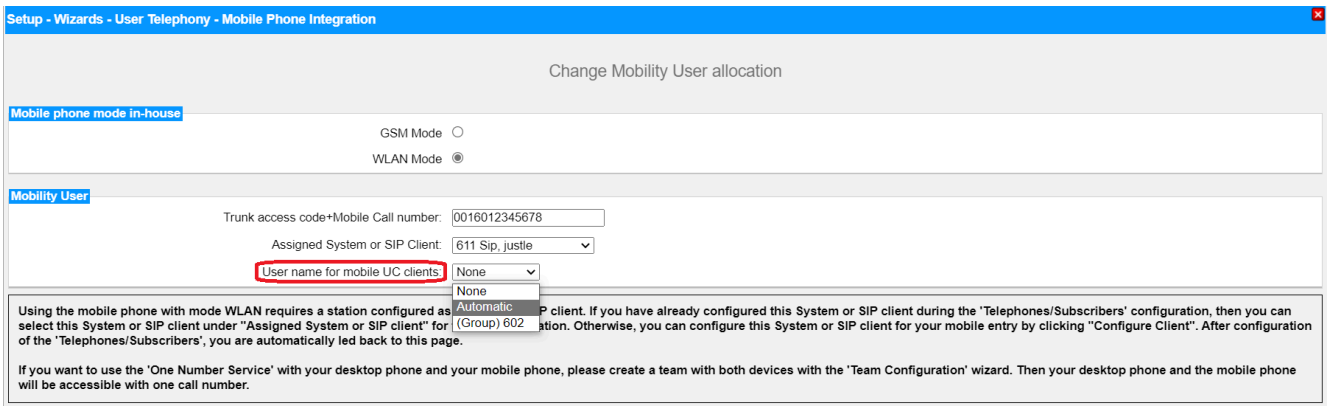


NOTICE: DISA is required for Mobility Entry (to control the system using DTMF) and for myPortal for Mobile (only when using Call Through).

5) Click on **Add** or **Edit** for the appropriate subscriber whose GSM mobile phone is to be integrated into the communication system. The **Assign Mobility Stations** window appears.
6) Select **WLAN Mode** as the mode for your mobile phone operation.
7) Under **Trunk access code+Mobile phone number**, enter the phone number of the mobile phone (e.g., 0016012345678).
8) Select **Assigned System- or SIP Client** from the drop-down list.

   If the assigned system (HFA client) or SIP client is not yet configured, click on **Configure Client** and set up a system or SIP client. After the system

or the SIP station configuration, you will be automatically returned to this page.



9) In the **Username for myPortal to go (Web Edition)** drop-down list, select the corresponding SIP or HFA device. **If you select Automatic**, the internal number of the user will be used as the user name.
10) Click **OK & Next**.
11) Click **OK & Next** followed by **Finish**.

19.2.7.3 How to Enable the Web Interface for Mobile Phones and Web Clients

Prerequisites

You are logged into the WBM with the **Expert** profile.

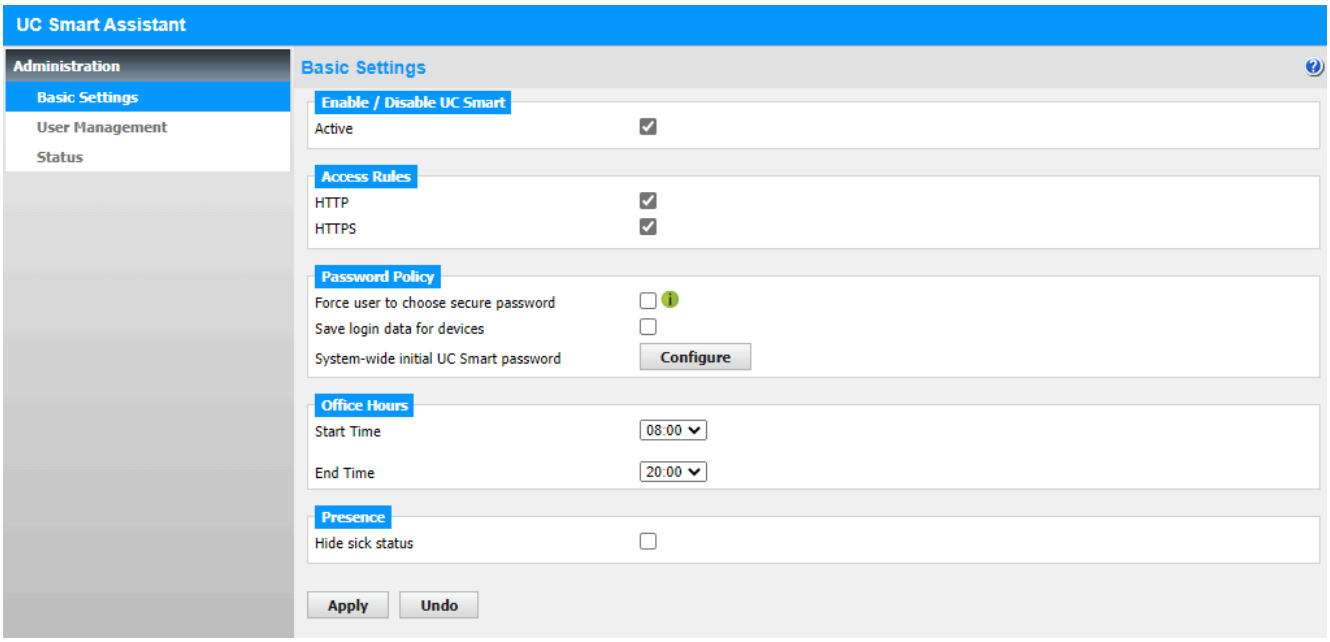
Web services must be enabled as a prerequisite for the following features:

- Mobile Phone Integration
- Application Launcher

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) If you are using UC Smart, click in the navigation tree on **Applications** > **UC Smart** > **Basic Settings**.
3) Make sure that UC Smart is **Active**.

4) If you want to enable web services for mobile phones, select at least one of the following options:
   - If you want to enable encrypted connections, select the check box **HTTPS**.
   - If you want to enable unencrypted connections, select the check box **HTTP**.



NOTICE: For security reasons, it is strongly recommended that only an encrypted connection (HTTPS) be used when working with myPortal to go (Web Edition) over the Internet.

5) Click on **Apply** followed by **OK**.

19.2.7.4 How to Delete Mobile Phone Integration

Use the **Mobile Phone Integration** wizard to delete the integration of the mobile phone.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **User Telephony**.
3) Click on **Edit** to start the **Mobile Phone Integration** wizard. The **Select Station for Mobility** window appears.
4) Click on **Edit** for the appropriate subscriber you want to delete. The **Assign Mobility Stations** window appears.
5) Click in the window below on **Delete Data**.
6) Click on **OK & Next**.

7) Click on **OK & Next** followed by **Finish**.

19.3 Mobility in the office

Mobility in the office is achieved via Desk Sharing, Cordless Phones and WLAN phones. For Desk Sharing, IP Mobility (Mobile Logon and Flex Call) offers features for mobile users who want to use the phone at a different workplace just like their own phone.

19.3.1 Desk Sharing

With Desk Sharing, multiple subscribers can share one system telephone and thus one IP phone (HFA).

With Desk Sharing, subscribers have no fixed workplace and no fixed office telephone. Desk Sharing enables multiple mobile subscribers of the communication system to share an office workplace and/or the phone. The subscriber simply logs in at the workplace phone where he or she happens to be currently working.

After the login, the station number of the logged in subscriber is transferred to the used system telephone. The used system telephone can no longer be reached under its original station number. If the subscriber logs in at another system telephone, his or her station number is transferred to that new system telephone. When the user logs out (Logout), the system phone automatically logs back on with its own non-mobile number.

One of the following steps must be performed at the system phone to activate the feature:

- Enter code for "mobile logon" + number of mobile station + optional password/PIN

When using phones with different numbers of function keys, the transfer of key layouts may be subject to restrictions.

If Desk Sharing is to be implemented for IP telephones (HFA) in networked nodes, an external DLS (Deployment Service) must be installed. The required expertise for this purpose is assumed.

The following features can be used for Desk Sharing:

- Speaker call (paging)
- Conferencing
- Override
- Toggle/Connect
- Parking
- Consultation
- Transfer
- Call pickup
- Do not disturb
- Call forwarding
- Send message (message waiting)
- Callback

- Station number suppression
- Ringing group on

NOTICE: For each mobile phone number, an additional Deskshare license is required. This Deskshare license must be activated for the subscriber, and the subscriber must be configured as **mobile**. In addition, the Relocate feature must be enabled.

A system telephone that is used for Desk Sharing does not necessarily require a license. However, if no license is activated and no Desk Sharing subscriber is logged in, not even emergency calls will be possible from this phone. The system telephone/subscriber must be configured as **Non-mobile**.

If a system telephone is not to be used for Desk Sharing, it must be configured as **Non-mobile and blocked**.

NOTICE: Desk Sharing feature must not be used with the fist two active system stations.

19.3.2 Integrated Cordless Solution

OpenScape Business Cordless is the integrated cordless solution for operating cordless telephones (DECT phones) via the communication system. The HFA features of OpenScape Business can then be used with the connected DECT phones.

In the integrated cordless solution, the DECT phones are internal, system-specific stations as opposed to separate DECT systems, which are connected via standard interfaces.

The connection of OpenScape Business base stations for the operation of DECT phones can be implemented via:

- For OpenScape Business X1/X3/X5: direct connections to the $U_{P0/E}$ interfaces of the mainboard of the communication system (DECT Light)
- For OpenScape Business X3/X5: connection to the $U_{P0/E}$ interfaces of an SLU8N/SLU8NR board (DECT Light)
- For OpenScape Business X8: connection to the $U_{P0/E}$ interfaces of an SLMUC (SLMU + CMAe)

The Cordless radio technology corresponds to the DECT (Digital Enhanced Cordless Telecommunications) Standard. The entire radio area administered by the system is made up of base stations, which together form either a complete network of overlapping radio cells or individual radio "islands". The size of a radio cell is dependent on the local/structural factors.

ECO Mode

In ECO mode (economic mode), the transmit power of DECT phones is either reduced by a fixed value (static) or every DECT phone adjusts its transmit power independently to the received signal strength (adaptive). ECO mode can be enabled at the communication system on a system-wide basis for all DECT phones (**Expert Mode** > **Telephony** > **Cordless** > **System-wide**). No

configuration is required at the DECT telephones. A manual system restart is needed to activate the feature in case of OpenScape Business X1, X3, X5.

- Static adjustment of transmit power

  The DECT phones and base station reduce the transmit power to a set fixed value.
- Adaptive adjustment of transmit power

  The DECT phones transmit with normal or reduced transmit power, depending on the reception field strength. During a handover, the system first switches to the high transmit power and then reduces the transmit power, depending on the reception.

DECT phones

The integrated Cordless solution supports GAP-enabled mobile telephones from third-party manufacturers. The full scope of HFA services can, however, only be used with approved DECT phones.

Configuration

For a description of the configuration, see Configuring the Integrated Cordless Solution.

Boards and Base Stations

The descriptions of the boards and base stations can be found in the found in the *OpenScape Business Service Documentation in chapters Boards and Base Station*.

19.3.2.1 System Overview

The connection of the OpenScape Business base stations for OpenScape Business X3/X5 occurs either directly at the $U_{P0/E}$ interfaces of the mainboard or at the UP0/E interfaces of an installed SLU8N/SLU8NR board (DECT Light). With OpenScape Business X8, the base stations can be connected to the Cordless SLMUC boards.

Direct Connections (DECT Light)

The base stations can be connected directly to the $U_{P0/E}$ interfaces of the OCCM, OCCMB, OCCMA and OCCMR, OCCMBR, OCCMAR of the OpenScape Business X3R/X3W and OpenScape Business X5R/X5W communication systems or to the UP0/E interfaces of an SLU8N/SLU8NR8 board.

By using the CMAe subboard on the mainboards the ADPCM conversion and echo cancellation functions (48 channels for CMAe) are made available. Up to four calls an be conducted per base station. Up to seven base stations can be connected to the $U_{P0/E}$ interfaces of the mainboards OCCM, OCCMB, OCCMA and OCCMR, OCCMBR, OCCMAR.

If no CMAe is installed, a maximum of two calls can be conducted per base station. In this case, the ADPCM conversion is performed directly by the DECT base station.

NOTICE: In case of no CMAe is installed no echo handling functions are available.

When connecting base stations to an SLU8N/SLU8NR board, the following connectivity requirements apply:

- In total, a maximum of 15 base stations (7 at the mainboard and 8 more at an SLU8N/SLU8NR board) can be operated. The maximum number of connectable DECT telephones is 64 with a CMAe.
- Only one SLU8N/SLU8NR board can be used for the connection of base stations.
- Only the first port on the base station can be used to connect of the base station to a $U_{P0/E}$ interface of the SLU8N/SLU8NR board. The ports 2 and 3 of the base station are not supported for connection to a further $U_{P0/E}$ interface.
- The $U_{P0/E}$ interfaces of the SLU8N/SLU8NR board can be used with a mixed combination of base stations and/or telephones.

Connecting Cordless Boards

The base station BS5 can be connected to the $U_{P0/E}$ interfaces of the following Cordless boards:

- SLMUC (SLMU + CMAe) with OpenScape Business X8 (see *Service Documentation SLMUC chapter*)

  The connection of the base stations can be made via one, two or three $U_{P0/E}$ interfaces. The last 8 interfaces of an SLMUC can only be used as 2nd or 3rd UP0 interface of the base station. The additional connection of $U_{P0/E}$ interfaces increases the traffic capacity of the base station and thus the number of simultaneously available voice channels.

19.3.2.2 System Configuration

Depending on the communication system, up to 64 base stations can be connected, and up to 250 DECT phones can be used.

The following table shows the maximum possible system configuration for the integrated cordless solution.

NOTICE: The base stations BS4 (S30807-U5491-X), BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) and BS3/S (X30807-X5482-X100) are being phased out and can no longer be ordered. However, they can still be connected to OpenScape Business X communication systems. In the event of a failure, the current base stations should be used.

NOTICE: If no CMAe is installed, a maximum of two calls can be conducted per base station. In this case, ADPCM conversion is performed directly by the DECT base station,but echo cancellation is not directly supported. In case that echo cancellation is required a CMAe subboard is needed .

OpenScape Business	Maximum number of boards		Clock Module	Max. number of Base Station BS when connected via 1xUp_0	Ports/ Simultaneous calls per BS	Max. number of registered devices	Max. number of simultaneous calls
	SLUN	SLMUC					
X1	-	-	-	7	1/2	16	14
	-	-	CMAe	7	1/4	16	16
X3	-	-	-	7	1/2	32	14
	-	-	CMAe	7	1/4	64	28
	1	-	CMAe	15	1/4	64	48
X5 Onboard $U_{P0/E}$ (SLUC)	-	-	-	7	1/2	32	14
	-	-	CMAe	7	1/4	64	28
	1	-	CMAe	15	1/4	64	48
X8	-	4	CMAe	64	3/12	250 (128 per SLMUC)	192[9]

NOTICE: The designation SLUC in the table refers to the UP0/E interfaces of the mainboard. SLUN generally refers to the SLU8N or SLU8NR boards.

19.3.2.3 Cordless/DECT Phones

Inserting the SLC board and entering the DECT system ID will automatically configure 16 handsets. The handset codes (PIN) are allocated and the handsets can be registered. Any additional handsets must be released before they can be used.

If a handset is replaced for servicing, the PIN must be changed before logging on the replacement handset. When a handset is replaced, a new PIN must be assigned to the relevant station in the communication system. This ensures that the handset is automatically logged off. It also improves security by preventing unauthorized parties from misusing the old PIN to log on the mobile handset.

19.3.2.4 Significance of Results Obtained from Testing the Radio Area

IMPORTANT:

Values recorded with a mobile telephone are not very precise and are intended to provide a rough assessment only. In addition, different values may be recorded on each mobile telephone even though the ambient conditions are identical. If you require more accurate results, we recommended that you use the Hicom Cordless Service tool (HCS-DECT).

9 The max. value per SLMUC is 48. Depending on the location of the cordless telephones in case of roaming, all devices that are registered (250) could be active if 4 SLMUC are available.

The following figure shows a sample display of the measuring results for a Gigaset mobile telephone when a call is in progress:

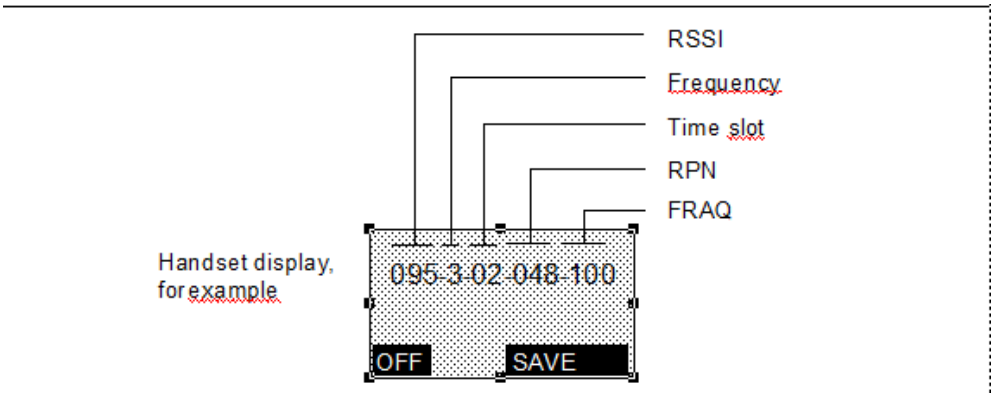


Figure 8: Measurement result

Section	Description
RSSI (radio signal)	Field strength of the radio signals received from the base station, normalized to a maximum of 100. If the value is < 50, the radio connection to the base station is no longer guaranteed. Acceptable field strength is > 50 (> -60 dBm).
Frequency	Frequency (0 – 9)
Time slot (Slot)	Time slot (0 – 11) of the receiving channel on which the measurement is carried out.

Section	Description
RPN (port number)	**OpenScape Business X1/X3/X5/X8** Base station ID, for example, 048, port number in the SLC boards. If the handset switches to an overlapping radio cell/base station, the current port number (where the D channel of the base station is configured) is shown on the handset display. Formula: A x 16 + B A = number of the SLC board (1 - 127); 16 = factor B = port of the associated SLC board (where the D channel of the base station is configured) Examples: RPN = 1 x 16 + port 0 = 016 RPN = 2 x 16 + port 8 = 040. The Port Number (PRN) is displayed for the Gigaset S3 professional and Gigaset SL3 professional handsets in hexadecimal format with an appended H. The hexadecimal value is shown without an appended H, e. g. "-028-" in the case of the Gigaset S4 professional and OpenStage SL4 professional handsets. Example: If the value 040 was displayed previously, the value 028H is now displayed for the Gigaset S3/SL3 professional. The hexadecimal notation is differentiated uniquely on the basis of the "H" suffix. This is also valid for OpenScape DECT Phone S5/SL5/S6/SL6/R6 devices (prefix H is not present).
FRAQ(frame quality)	Transmission quality in %. 95 % to 100 % satisfactory (for short periods 90 % to 94 % non-critical), < 95 % faulty.

For more information regarding the measurement menu, see: *OpenScape Cordless Enterprise, Service Documentation, Chapter: Testing the Radio Area* and *OpenScape Business X3/X5/X8, Service Documentation, Chapter: Check the Radio Coverage.*

19.3.3 Configuring the Integrated Cordless Solution

The configuration of the integrated Cordless solution includes setting up the base stations and the registration of DECT phones / mobile handsets at the communication system.

The configuration is performed in Expert mode.

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). The DECT phones are charged. The DECT system ID is known. Information about subscribers, station numbers, names and, if necessary, their allocation to the SLC board is available.

General Process for Configuring the Integrated Cordless Solution

1) Configure the DECT system ID and other Cordless parameters, if necessary
2) Configure Cordless base stations
3) Log on the DECT phone at the Cordless base station
4) If necessary, add more DECT phones as required.

After the DECT phones have been commissioned, the phone numbers and names and other settings of the DECT subscribers can be edited via the WBM with the **Telephones/Subscribers** wizard.

DECT System ID

The DECT system ID is used to distinguish the different DECT systems and thus to identify the radio signals. Specifying the DECT system ID is necessary for synchronizing the registered handsets with the system.

The DECT system ID is an 8-digit hexadecimal string that is supplied on purchasing the DECT system. It is valid throughout the system (even for maintenance and service).

The DECT system ID consists of:

Digit	Meaning
1st. digit	E/ARC (Access Right Code)
2nd. - 5th. digits	EIC (Equipment Installers Code)
6th. - 7th. digits	FPN (Fixed Part Number)
8th. digit	FPS (Fixed Part Subscriber)

19.3.3.1 How to Configure the DECT System ID and Other Cordless Parameters (System-wide Data)

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

The 8-digit DECT system identifier supplied with the ordered DECT system is available.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Cordless** in the navigation tree.
3) In the menu tree, click on **Cordless** > **System-wide**.
4) Enter the 8-digit DECT system identifier under **System ID**.
5) The system-wide settings under **Echo Handling** and **Economic Mode** should only be only if required. An explanation of the settings can be found under Cordless>System-wide.
6) Click on **Apply**, followed by **OK**.

19.3.3.2 How to Configure Cordless Base Stations

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Cordless** in the navigation tree.
3) In the menu tree, click on **Cordless** > **Base Stations**. All connected base stations are displayed.
4) If one or more base stations are connected directly (without SLC board) to the system (SLUC), you can enable or disable the base stations via the **Type** selection list:
   a) **Base station**: The base station is activated, and 16 DECT phones and one SLC networking line are automatically preconfigured.
   b) **No Port**The base station is deactivated with all associated DECT phones and the SLC networking line.
5) If required, edit the preconfigured name of the base station (e.g., `Base 1`) under **Name**.
6) Specify the level for the base station (50% or 100%) under **Level**.
7) Click on **Apply** followed by **OK**.

19.3.3.3 How to configure DECT Phones for the First Time

Prerequisites

You are logged into the WBM with the **Expert** profile or you are using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

The following configuration steps should be done before registering DECT devices to the system.

Step by Step

1) Perform the following steps, if you are using WBM:
   a) In the navigation bar, click on **Expert Mode**.
   b) Click on **Telephony** > **Cordless** in the navigation tree.
   c) In the menu tree, click on **Cordless** > **SLC**. All DECT phones already configured are displayed. When connecting a base station, 16 DECT phones are automatically preconfigured.
   d) If required, edit the preconfigured internal call number of the DECT phone under **Call No**.
   e) If required, edit the preconfigured direct inward dialing call number of the DECT phone under **DID**.
   f) If required, edit the preconfigured name of the DECT phone under **Name**.
   g) If required, edit the preconfigured mobile code (PIN) of the DECT phone under **Mobile code**. This code must be entered at the DECT phone when logging into the base station for the first time.
   h) Click on **Apply** followed by **OK**.
2) Perform the following steps, if you are using Hipath 3000 Manager:
   a) Upload the KDS database checking **Read/Write Database** and **System > PC**
   b) In the menu tree go on **Settings > Cordless** in the navigation tree.
   c) In the menu tree, click on **Cordless > SLC** then on the parameter **Portable parts** check all. All DECT phones already configured are displayed. When connecting a base station, 16 DECT phones are automatically preconfigured.
   d) If required, edit the preconfigured internal call number of the DECT phone under **Call Number**.
   e) If required, edit the preconfigured name of the DECT phone under **Name**.
   f) If required, edit the preconfigured mobile code (PIN) of the DECT phone under **Mobile code**. This code must be entered at the DECT phone when logging into the base station for the first time.
   g) Click on **Apply** followed by **OK**.
   h) Transfer the KDS to system, if any change have been made.

Related tasks

How to Configure DECT Stations on page 441

19.3.3.4 How to Register a DECT Phone (OpenStage/Gigaset Handset) at the Cordless System

Before registering a DECT phone on, you must use a system telephone and open the registration window with the DECT registration code. Then, enter the station numbers of the DECT phones that you want to register. A maximum of 10 station numbers can be registered in the same registration window. A registration window is open for up to 10 minutes.

If no system phone is available, then you can use Hipath 3000 Manager **Online** feature and make the actions from there instead of using a physical phone. Below steps refer to the physical telephone.

Below steps refer to the physical telephone.

Step by Step

1) Open the registration window at the communication system:
   a) On the physical phone enter the code *94 2 then 19970707.
   b) Enter the station numbers of the DECT phones that you wish to register.

2) Register the DECT phone:
   a) From the DECT phone from home screen, press the **menu key**.
   b) Navigate to **Settings > Registration > Register Handset** and select **Base**.
   c) You will be asked to enter the Station system PIN. Enter the eight-digit mobile telephone code and confirm your entry.

      You must wait one or two silent calls, which means short automatic calls (on some devices this is like 2 rings).

      If you are registering an inactive call number (which has not been used before, it looks black at WBM and gray in KDS) then the registration is completed with one silent call. If you are registering an active call number that has been used before (looks green at WBM and KDS) then the registration is completed with two silent calls.

      Please do not take any further action (e.g. initiating DECT phone calls) until this process is complete!

On successful registration, you will see the station number in the Home Screen and you will be able to use the device.

Example: Registering the mobile telephone (station number 125) to DECT telephone system using the mobile telephone code (PIN) 11112345 (which has been configured as a mobile code via Manager E or using WBM- as was mentioned on the chapter: How to configure DECT Phones for the First Time on page 922.)

1) Activate the Registration window from a physical phone connected to the system entering *942.
2) You will view on the display of the phone: **Code**.
3) Enter 19970707 and you will view on the display of the phone: **Tel. no**: Enter 125.
4) If needed, switch On the mobile telephone by pressing the on-hook key for longer than one second. You will then hear a confirmation tone.
5) You must make the following entries within ten minutes. Press the menu key.
6) Navigate to **Settings** of the phone menu and confirm.
7) Navigate to **Registration** and confirm the first choice: **Register Handset** (do not select the second option: Select Base)
8) Select a station (in this example **Base 2**) and confirm. You will view in the middle of the display **Registration** and **Please enter system PIN**.
9) Enter the eight-digit PIN (mobile telephone code; in this case, **11112345**) and confirm your entry. If registration is successful, you have to wait for a “silent call”, which means a short automatic call (on some devices this is like 2 rings). If you are registering an inactive call number (which has

not been used before, it looks black at WBM and gray in KDS) then the registration is completed with one silent call. If you are registering an active call number that has been used before (looks green at WBM and KDS) then the registration is completed with two silent calls. Please do not take any further action (e.g. initiating DECT phone calls) until this process is complete! Then on the left side of the screen you will see Base 2 (in this case). After this, you will view the station number (125) at your Home Screen.

10) You can change the name Base 2, if needed. To do this, navigate to Settings and confirm, go to Registration and confirm and then choose the second option Select Base. Select the Base name which has to be renamed, pressing **Name**, and rename the base name (for example renaming it to 125).

19.3.3.5 How to Add Additional DECT Phones

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click on **Telephony** > **Cordless** in the navigation tree.

3) In the menu tree, click on **Cordless** > **SLC**.

4) Click on the desired board in the menu tree.

5) Click on the **Add DECT Stations** tab.

6) Enter the number of newly added DECT phones under **Number of DECT phones**. The newly added DECT phones are displayed under the **Edit DECT Stations** .

7) Click on **Apply**, followed by **OK**.

19.3.3.6 How to Delete DECT Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

DECT phones are configured.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click on **Telephony** > **Cordless** in the navigation tree.

3) In the menu tree, click on **Cordless** > **SLC**. All DECT phones already configured are displayed.
4) Select the DECT phones to be deleted in the **Delete** column.
5) Click **Apply**, followed by **OK**.

19.3.3.7 How to Configure the Multi-SLC Parameters

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

There are multiple SLMUC boards inserted in the OpenScape Business X8.

An OpenScape Business base station is connected to the communication system.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Cordless** in the navigation tree.
3) In the menu tree, click on **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.**

      Range of values: 1-15,17-31,33-47,...,127. Multiples of 16 are not allowed.
   b) If required, edit the preconfigured system-wide unique call number of the SLC networking line of the SLMUC board under **SLC number**.

      NOTICE: For each SLC networking line, an internal S_0station is set up. The SLC call number corresponds to the number of internal S_0 station.
   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) Click on **Apply** followed by **OK**.

19.3.3.8 How to Query the Data for Base Stations

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Cordless** in the navigation tree.
3) In the menu tree, click on **Cordless** > **Base Stations**.
4) Click on the desired base station in the menu tree. The data of the base station is displayed. An explanation for the data can be found under Cordless>Base Stations.
5) You can select up to 10 different frequency channels simultaneously for a base station. An explanation of the frequency channels can be found in the table under Cordless>Base Stations.
6) Click on **Apply**, followed by **OK**.

19.3.3.9 How to Enable the Message Waiting Indication (MWI) for DECT Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click in the navigation tree on **Telephony Server** > **Basic Settings**.
3) In the menu tree, click **Basic Settings** > **System** > **System Flags**.
4) Select the **CMI MWI ringer** check box in the **System flags** area.
5) Click on **Apply**, followed by **OK**.

19.3.3.10 How to Check the Logon Status of DECT Phones

Prerequisites

You are logged into the WBM with the **Expert** profile, or Hipath 3000 Manager. Below steps refer only to WBM, but similar actions can be performed using Hipath 3000 Manager.

An OpenScape Business base station is connected to the communication system.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Cordless** in the navigation tree.
3) In the menu tree, click on **Cordless** > **SLC**. All DECT phones already configured are displayed.

4) For each DECT phone, the login status is displayed in the **Active** column as follows:
   - Green: The mobile phone is active.
   - Red: The board lockout switch was set for a logged-on mobile phone.
   - Yellow: The mobile phone was automatically logged off on changing the PIN.
   - Gray: No mobile phone has ever been logged on at this port.
5) Click on **Apply**, followed by **OK**.

19.3.4 Cordless IP

Cordless IP (IP DECT) is the optional Cordless solution that serves as an alternative to the integrated Cordless solution or is used with OpenScape Business S.

The DECT phones at Cordless IP communicate via the BSIP base station with the communication system like SIP phones. Consequently, only SIP features can be used with Cordless IP. For more information on Cordless IP, refer to the documentation for HiPath Cordless IP.

For all SIP subscribers who are logged on at a Cordless IP, the station parameter **autom. connection, CSTA** must be disabled. Otherwise, this could cause calls between SIP subscribers to not be set up via DECT IP.

19.3.5 WLAN Phones and Access Points

WLAN phones and dual-mode telephones enable mobile communications. These phones can be integrated in already existing WLAN infrastructures. With WLAN Access Points, you can build wireless networks and use the same infrastructure for voice and data services. It is only recommended that only high-performance WLAN Access Points (e.g., from Enterasys) be used.

19.3.5.1 WLAN Requirements

When using a WLAN, it is important to ensure that the basic requirements for Voice-over-WLAN are satisfied. To implement the wireless portion of the network, a site survey may need to be conducted.

Decision-making aids:

- Smaller installations with up to three APs can be effectively assessed during a site visit or by studying the floor plans. It is not generally necessary to perform a site survey in this scenario.
- Site surveys should always be performed for installations with more than four APs. This applies specially to installations extending across multiple buildings or floors within buildings.
- A site survey is required irrespective of the number of APs in scenarios involving an RF-intensive environment or if you want the solution to operate alongside preexisting WLAN systems.

19.4 Mobility at Home

Mobility at Home is achieved through teleworking. This is done by integrating non-local phones (such as a home phone or mobile phone) in the OpenScape Business communication network.

The following types of teleworking stations are available:

- VPN stations

  OpenScape Business has a built-in VPN functionality. A total of 10 teleworkers can be simultaneously active via VPN. This may involve a home PC or a mobile phone with an Android or iOS operating system. The VPN connection is established between the native VPN client of the PC or of the mobile phone and the OpenVPN server of OpenScape Business.

  Users of UC Suite can specify their home phone number from home via their UC client and then use their private phone as an office phone (CallMe).
- Device@Home: SIP@Home stations or System Device@Home stations

  STUN-enabled SIP phones (e.g., Yealink T19) (SIP Device@Home stations) or HFA phones (System Device@Home stations) can register themselves at the communication system over the Internet by using the internal SBC function of OpenScape Business. To do this, the feature must be enabled in the station data for each SIP phone or HFA phones via the WBM.

  A STUN server must be additionally specified in the WBM only if no ITSP is being used or if the used ITSP does not offer any STUN server.

  SIP Device@Home does not support the transmission of video signals.

NOTICE: When using multiple SIP/HFA @Home devices behind the same router, NAT limitations may cause call payload issues due to port reuse conflicts; to avoid this, configure each device with a unique source (RTP) port.

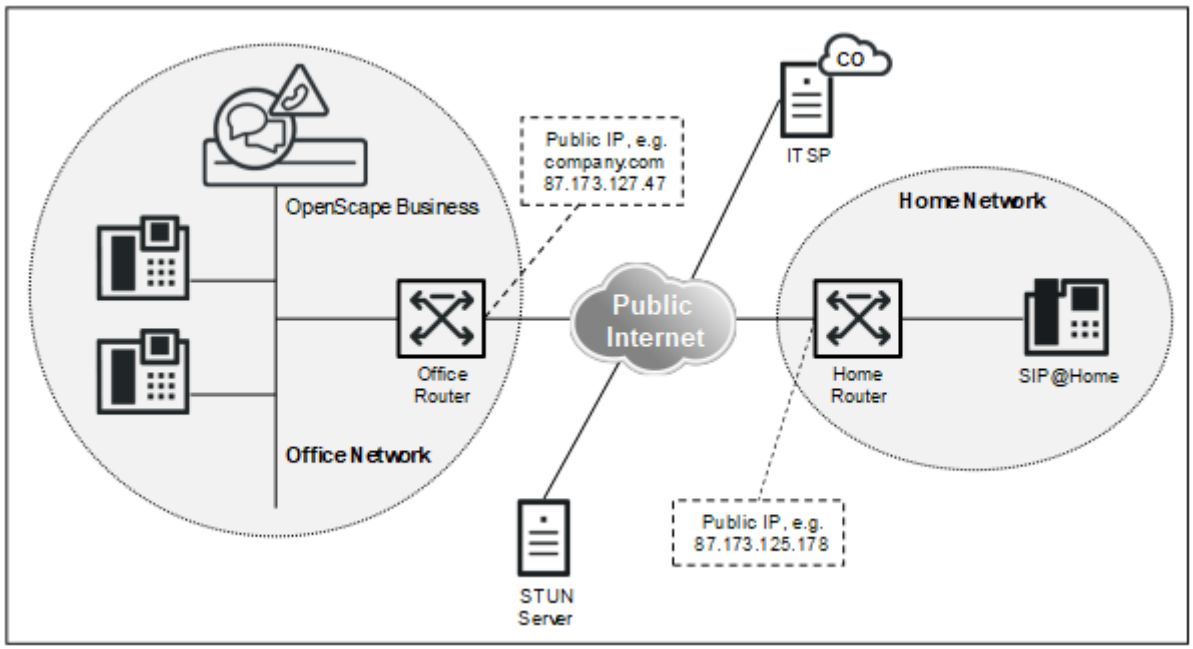


Figure 9: Device@Home (SIP Device@Home or System Device@Home) components

19.4.1 Configuring a VPN

In order to connect subscribers to the communication system via the integrated VPN functionality, certain configurations must be performed at both OpenScape Business and the VPN stations.

Configuring OpenScape Business

For the VPN configuration of the communication system, see How to Connect Teleworkers via a VPN .

Configuring VPN Stations (VPN Clients)

To configure the VPN client, see VPN Clients .

19.4.2 Configuration for SIP Device@Home

In order to set up connections from a STUN-enabled SIP phone to OpenScape Business over the Internet, certain configurations must be performed.

Configuring OpenScape Business

In order to enable a SIP station to register at the communication system over the Internet, the integrated SBC function must be activated for the SIP station (see How to Enable Device@Home).

The integrated SBC function detects the public IP address of the communication system and the port used with the aid of the STUN protocol. If the communication system is connected to an ITSP that offers a STUN server, no further configuration must be performed on the communication system. However, if either no ITSP is used or if the used ITSP does not offer any STUN

server, then a STUN server must be configured in the system (see How to Specify a STUN Server for Device@Home).

Configuring the Office Internet Router

In order to enable SIP phones to reach the communication system over the Internet, port forwarding for the external SIP port must be set up in the Office Internet router. To prevent SIP attacks from the Internet, a SIP port other than the default must be used as an external SIP port.

The transport protocol is set at the SIP phone.

Table 9: Configure Port Forwarding in the Office Router

Transport protocol	Internal SIP port	External SIP port	Comment
UDP	5070	Entering 5090, for example.	For port forwarding, the external and internal SIP ports must not be the same. A port with a different value than the internal default SIP port 5070 can thus be entered as an external SIP port. UDP is therefore recommended.
TCP	5070 Switching to 5080, for example	Entering 5080 (= internal SIP port), for example	For port forwarding, the external and internal SIP ports must be the same. To use an external SIP port other than the default 5070, the internal SIP port must be changed. This requires a reconfiguration of all IP components that use SIP. TCP is therefore **not** recommended.
TLS	5071	Entering 5071 (= internal SIP-TLS port)	For port forwarding, the external and internal SIP-TLS port must be the same. Since the internal SIP-TLS port already differs from the default SIP-TLS port, 5071 can also be entered as the external SIP-TLS port. TLS is therefore recommended.

NOTICE: In an upgraded system no change regarding SIP ports is performed automatically. After upgrade the ports are:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

These values must be changed manually by the administrator if Device@Home is used in a migrated system.

For TLS, valid certificates must be enabled in the communication system. TLS connections for SIP stations are supported at the LAN interface of the communication system, but not at the WAN interface. SRTP payload with SDES signaling is not supported.

If the Office Internet router is connected to the Internet without a fixed IP address, then DynDNS must be configured at the Office Internet router so that SIP stations can reach the communication system over the Internet. The current IP address is registered via the DynDNS account at regular intervals. With free DynDNS accounts, which expire at regular intervals, this may temporarily lead to disruptions.

Configuring SIP Phones

As an example for the configuration you can find some tested SIP phones that support STUN, please refer to the Unify Experts wiki on the Internet. You will find the values that need to be entered at the SIP phone there.

Configuring the Home Internet Router

No special configuration is needed on the home Internet router.

The home Internet router must meet the following requirements:

- The router must provide VoIP functionality with NAT enabled (not a symmetric NAT).
- The ALG function must be disabled in the router.

The Internet connection must provide enough bandwidth for the transmission of the call. For asymmetric DSL connections, in particular, the availability of sufficient upload bandwidth must be ensured.

Configuring myPortal @work

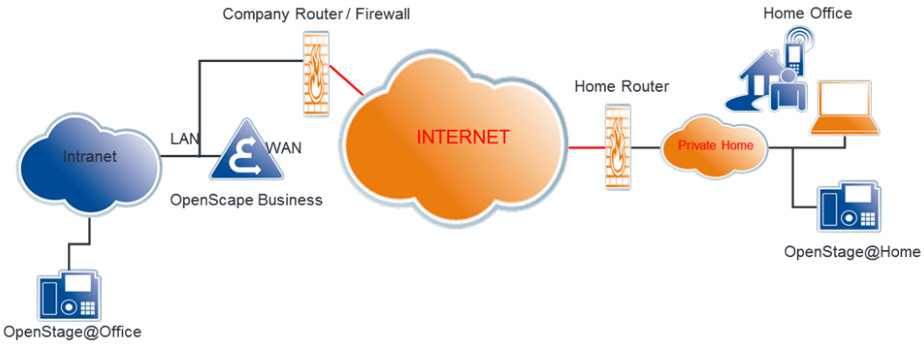
In order to enable myPortal @work to reach the communication system over the Internet, you have to perform the following:

- Configure the STUN server to the system/client.
- Open and forward port 8802 (no other forwarding is required).
- The SBC flag is not needed . Based on WebRTC, the integrated SBC function is not required to be activated.

19.4.3 Configuration for System Device@Home

In order to set up connections from a System Device phone to OpenScape Business over the Internet, certain configurations must be performed at OpenScape Business, the office Internet router and the System Device phone.

- **Figure 10: Example of System Device@Home use case**



Configuring OpenScape Business

In order to enable a System Device@Home station to register at the communication system over the Internet, the integrated SBC function must be activated for the System Device@Home station (see How to Enable Device@Home on page 934).

The integrated SBC function detects the public IP address of the communication system and the port used with the aid of the STUN protocol. If the communication system is connected to an ITSP that offers a STUN server, no further configuration must be performed on the communication system. However, if either no ITSP is used or if the used ITSP does not offer any STUN server, then a STUN server must be made known to the communication system (see How to Specify a STUN Server for System Device@Home).

Configuring the Office Internet Router

In order to enable System Device@Home stations to reach the communication system over the Internet, port forwarding for the System Device port must be set up in the Office Internet router. To be able to register from the Internet, the office router/ firewall must be configured with a port forwarding rule:

- external port TCP/4060 to internal port TCP/4062(HFA), for non-TLS

  external port TCP/4061 to internal port TCP/4063(HFA), for TLS

  NOTICE: During migration from V2R1 to a higher version, the office internet router should also reconfigured according to this rule.

  Above mentioned ports are only needed for System Devices (HFA Phone).

- RTP port range in OpenScape Business X:30274-30529RTP port range in OpenScape Business S: 30528-30887 (default values)

  VoIP enabled UC Clients such as myPortal to go, myPortal @work do need these ports as well.

- TCP/8802 (HTTPS) (required for Unified Communications client (e.g myPortal to go, myPortal to go Web, my Portal @work or VoIP for myPortal to go configured as System Device@Home)

  NOTICE: The internal firewall zone must be closed.

The transport protocol is set at the System Device@Home station.

If the Office Internet router is connected to the Internet without a fixed IP address, then DynDNS must be configured at the Office Internet router so that System Device@Home stations can reach the communication system over the Internet. The current IP address is registered via the DynDNS account at regular intervals. With free DynDNS accounts, which expire at regular intervals, this may temporarily lead to disruptions.

Configuring the Home Internet Router

No special configuration is needed on the home Internet router.

The home Internet router must meet the following requirements:

- The router must provide VoIP functionality with NAT enabled (not a symmetric NAT).
- The ALG function must be disabled in the router.

The Internet connection must provide enough bandwidth for the transmission of the call. For asymmetric DSL connections, in particular, the availability of sufficient upload bandwidth must be ensured.

Configuring the HFA Phone

The Gateway must be configured with the DNS name (e.g. mycompany.net) so that the phone can reach the system over the Internet. The IP of DLI is also needed to be configured. An internal phone number must be added for the subscriber. The device's password must also be set.

Restrictions

- It is not possible to configure XML applications at OpenStage

19.4.4 How to Enable Device@Home

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click **Stations** > **IP Clients** > **SIP Clients** or **System Clients**
4) Click on the desired SIP or HFA station in the menu tree.
5) Click the **Edit Workpoint Client Data** tab.

6) Make sure that a password is entered. The values specified here must also be entered on the SIP phone or System Device.

NOTICE:

A strong password should be used when connecting over the Internet (at least 8 characters including uppercase, numeric, and special characters).

NOTICE: The password of Deskshare clients which are declared as @Home should contain only numerical characters. This password is actually the pin code for the activation of the mobility feature (feature's service code: *9419). Devices support only numerical characters for pin.

After setting the password, the **Internet Registration with internal SBC** is available to be enabled.

NOTICE: After speed upgrade or system restart, Authentication active checkbox will be activated for all SIP endpoints and will be greyed-out so the user cannot disable it, if at least one SIP station has the **Internet Registration with internal SBC** flag activated.

19.4.5 How to update software for System Device (HFA) @Home

The normal SW-Update procedure of the DLI for an internally connected device cannot be used for System Device (HFA)@Home as this requires direct access to the IP address of the device for the file transfer. The DLI cannot determine the IP address of the System Device@Home due to the following reasons:

- The Device@Home resides in a home network using private IP addresses. Internet access is done via a Home Router with Network Address Translation (NAT).
- The DLI within OpenScape Business is located in a company/office network using private IP addresses. The company network is connected to the Internet via the Company/Office Router.

Therefore the DLI SW-Update procedure uses an additional HTTPS connection via port 8804 (default setting) in combination with the DLI port 18443 (default setting) to determine SW version of the Device@Home and to perform the SW-Update.

The SW-version check for a Device@Home is only done if one condition of the following applies:

- Device restart
- Configuration change locally or remotely
- Inventory changes of the device.
- Logon or logoff of a mobile user on a device.

In these cases the DLI checks the software version of the device and performs an SW update in case that a newer SW version is available in OpenScape Business.

Automatic software update of a Device@Home by the DLI has to be configured in OpenScape Business. It is disabled per default and needs to be enabled explicitly.

The following steps are needed.

Step by Step

1) You are logged into the WBM with the Expert profile.
2) In the navigation bar, click on **Expert Mode**.
3) Click **Telephony Server > Basic Settings** in the navigation tree.
4) Click on **Basic Settings > Phone Parameter Deployment** in the navigation tree.
   - Clicking on **Deploy SW to @Home devices**, permissions are given for software update via DLI for System Devices (HFA) @Home. The default value is 'unchecked'.
   - Click on **Apply** followed by **OK.**
5) Firewall Settings

   No manual firewall settings are required in OpenScape Business. The port 8804 is opened during system startup and requests that arrive at this port are answered only by the system if **Deploy SW to @Home devices** flag is enabled.
6) Open the used ports 18443 and 8804 for the DLI with the proper configuration (port forwarding) in the company/office router.

Limitations

The HFA@Home device resides behind a firewall (home router). The router or firewall induces a network address translation (NAT) and this makes IP address impossible to be visible from the outside world. As a result, IP phones can not be seen remotely in order to be administered by the DLI.

The side affect of the above network restriction is that any DLI driven events can not be accomplished, as these events are sent towards to the local (not accessible) IP address of the device.

The impact is that no on-demand software update will be possible. On the other hand, the software update will be possible when the device initiates a message exchange by opening an HTTPS session to DLI. Sessions are opened due to specific device-driven events, such as:

- the device restarts.
- a configuration change has been done on the device (via local display or web-based management).
- inventory changes of the device.
- logon or logoff of a mobile user on a device.

In all these cases, DLI will check the software of the device and if needed the device will be updated to the official software that OSBiz supports.

NOTICE: Software deployment takes place when the phone starts up (either when it gets registered to OSBiz, or when the OSBiz system comes in service).

19.4.6 How to Specify a STUN Server for Device@Home

Prerequisites

You are logged into the WBM with the **Expert** profile.

No ITSP is being used or the used ITSP does not provide any STUN server.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Voice Gateway**.
3) In the menu tree, click **Internet Telephony Service Provider**.
4) Click the **Edit STUN Configuration** tab.
5) Enter the IP address or the host name of the STUN server (e.g., `stun.serviceprovider.com`) under **IP Address / Host name** in the **Default STUN Server** area.
6) Enter the port of the STUN server (e.g., `3478`) under **Port** in the **Default STUN server** area.
7) Click **Apply**, followed by **OK**.

20 Security

Security involves protecting the communication system and the stored and transmitted data against unauthorized access. This can be achieved through access protection for the IP network (firewall) and encrypted transmissions (SSL VPN, for example).

Security Checklist

The aspect of secure communications has been taken into account in the default settings of the communication system. During the initial setup, the functions and settings may need to be adapted to the specific situation of the customer, and additional provisions may have to be made in the customer environment. In order to raise the awareness of security risks and to implement suitable measures to counteract them, a security checklist is provided in the product documentation. It is urgently recommended that this checklist be discussed with the customer during the initial setup and that all implemented measures be carefully documented.

20.1 Firewall

A firewall is a system of software and hardware components that restricts access to different networks in order to implement a security concept.

Firewalls are installed at the interfaces between individual networks and control the data flow between the sub-segments to prevent unwanted data traffic and only allow the desired traffic. Firewall are most frequently used to control traffic between a local network (LAN) and the Internet.

In any corporate network, a firewall isolates the internal LAN from the Internet.

The communication system provides integrated security functions. Different functionality is offered by OpenScape Business X and OpenScape Business S for this purpose.

OpenScape Business X provides the following features:

- Port Firewall / NAT (firewall between WAN port and LAN)
- Application Firewall (firewall for access to the communication system)

OpenScape Business S uses the Linux firewall.

20.1.1 Port Handling

Port handling is used for activating ports (port mapping, port forwarding) in the firewall of the integrated router of the OpenScape Business X.

Port Numbers

NOTICE: You should open ports only if it is absolutely necessary for a particular application!

Ports or services are required for communication via the protocols TCP and UDP because they allow multiple applications to exchange data simultaneously over a single connection.

The term firewall is generally understood as a port firewall (i.e., the blocking of individual services, or ports). The port firewall affects only the WAN port of OpenScape Business.

With OpenScape Business S, a port firewall can be enabled on the LAN port under Linux. With OpenScape Business X, the firewall on the WAN port is enabled in order to protect the internal network (LAN ports) against attacks from the Internet. If any specific ports/services need to be accessible from the Internet, they must be explicitly released (see Opening Ports). All ports/services for the functionality of OpenScape Business X are automatically released on the LAN port (into the internal network).

OpenScape Business S has only one LAN port (into the internal customer network) and is protected from the Internet by other components/routers in the customer network. In addition, the Server-internal Linux firewall is enabled. To provide the required OpenScape Business functionality, specific ports/services must be opened (to allow the phones to communicate with OpenScape Business S, for example). This is done automatically, but the administrator can disable individual services.

Port numbers can accept values between 0 and 65535 which is how they are assigned to the different applications. The ports between 0 and 1023 are referred to as 'well-known ports' and are permanently assigned by the IANA (Internet Assigned Numbers Authority). A list of these ports can be found under http://www.iana.org/assignments/port-numbers.

20.1.1.1 Opening Ports

If the system sets up the Internet access (via the WAN port), then, by default, the only communication allowed is from within the internal network (i.e., from the corporate network or the communication system itself) to the Internet and the associated response packets. Requests initiated from the Internet are blocked. This security setting can be bypassed by opening the port selectively to operate a Web server on the network, for example.

NOTICE: If the communication system is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, the communication system opens the relevant ports and keeps them open.

Port 5060 must likewise be closed If an external router or firewall is being used. The communication system is responsible for opening this port (if required).

20.1.1.2 How to Configure the Opening of Ports

The **Firewall** wizard can be used to open ports so that the communication system or PC on the LAN are accessible via the WAN port. The opening of ports entails the risk of access by unauthorized persons. Consequently, only the ports that are urgently needed should be opened.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Security**.
3) Click on **Edit** to start the **Firewall** wizard. The **Opening ports** window appears.
4) Select the check box **NAT Rule Active** in the row associated with the relevant application or required service for which you want to release ports.
5) Enter the data for the release in the **Global Port**, **Local IP Address**, and **Local Port** fields.
6) To open a port for a service that is not entered, click **Add** and fill in the **Description**, **NAT Rule Active**, **Global Port**, **Local IP Address** and **Local Port** fields.
7) Click on **OK & Next**.
8) Click on **Finish**.

20.1.1.3 Port Management

Port Management can be used to change some of the ports used by the communication system itself. This enables the network communication to be customized for each customer network even if the ports are already being used elsewhere.

If changes are to be made at the port administration, these changes must generally be made in all components (phones, systems, etc.) simultaneously in order to retain functionality.

20.1.1.4 How to Edit Global Port Management Settings

You can specify port numbers for the individual functions here.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Port Management**. The **Edit Global Port Management Settings** tab appears.
4) Enter the port for each respective function under **Port Number** or leave the default settings unchanged.
5) Click on **Apply** followed by **OK**.

20.1.2 NAT

NAT (network address translation) is a procedure for replacing one IP address in a data packet with another. The clients in an internal network use private IP addresses. As private IP addresses are not forwarded in a public network, you

can use NAT to map the private IP addresses to a public IP address. This gives internal clients access to the public network while masking the structure of the internal network with its private IP addresses and keeping it separate from the public network (for example, the Internet). NAT and NAT rules are needed for the opening of ports.

Address translation is performed at the gateway between an internal and a public network. NAT can run on an Internet router, a server or another specialized device. An Internet router can use NAT, for instance, to connect the internal network to the Internet.

The internal network appears on the Internet with only a single public IP address, which is assigned to the Internet router by the Internet Service Provider (ISP). All access attempts made from the internal network are routed via this official IP address with different port numbers. The Internet router replaces the private IP addresses with the official IP address assigned by the ISP. In the case of incoming data packets, the official IP address is replaced by the private IP addresses. The relevant port numbers are important for allocation. Only specially enabled private IP addresses can be reached directly from the Internet.

NAT rules

You can use NAT rules to define if private (local) IP addresses should be reached directly from the Internet. Individual NAT rules can be defined for this or the default NAT rules already set can be used for the services FTP Server, HTTP Server, etc. A total of 20 NAT rules can be defined. In order to use a NAT rule, the local address data of the client PC that will provide these services for the Internet must be entered, and the NAT rule must be activated. Multiple NAT rules can be configured together with the help of a NAT table editor. You can delete NAT rules that are no longer needed.

Ports

At startup, servers usually require the operating system to provide specific ports in order to accept connections. Typical examples include an HTTP server on port 80, an FTP server port 21, etc. Clients normally request the operating system for a random port in order to set up connections.

20.1.2.1 How to Configure a NAT Rule

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **Routing**.

3) Configure the NAT rule:

- If you want to define a new NAT rule, click on **NAT** in the menu tree and then on the **Add NAT** tab.
- If you want to edit an existing NAT rule, navigate in the **NAT** menu tree down to the desired NAT rule.

4) Enter a name for the NAT rule in the **Description** field. In the case of a standard NAT rule, this name cannot be changed.
5) Enter the IP address you want to enable for the client in the internal network in the **Local IP Address** field.
6) Enter the port number used by the internal client's application in the **Local Port** field.
7) Enter the port number used by the external communication partner's application in the **Global Port** field.
8) In the **Protocol** drop-down list, select the transport protocol (**TCP** or **UDP**) used by the application. The protocol cannot be changed in the case of a standard NAT rule.
9) Select the radio button **NAT Rule Active** if you want to apply the NAT rule.
10) Click on **Apply** followed by **OK**. The activated NAT rule is identified under the menu item **NAT** with a green symbol.

20.1.2.2 How to Configure NAT Rules with the NAT Table Editor

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation bar, click on **Telephony** > **Routing**.
3) In the menu tree, click on **Routing**.
4) Click in the **NAT** menu tree and then on the **NAT Table Editor** tab.
5) Configure the NAT rule:
   - If you want to define a new NAT rule, fill in the fields of the first row as described below.
   - If you want to edit an existing NAT rule, click in the desired field of the NAT rule and fill them in as described below.
6) Enter the IP address you want to enable for the client in the internal network in the **Local IP Address** column.
7) Enter the port number used by the internal client's application in the **Local Port** column.
8) Enter the port number used by the external communication partner's application in the **Global Port** column.
9) In the **Protocol** drop-down list, select the transport protocol (**TCP** or **UDP**) used by the application. The protocol cannot be changed in the case of a standard NAT rule.
10) To apply the NAT rule, enable the **Active** column with a check mark.
11) Enter a name for the NAT rule in the **Description** column. In the case of a standard NAT rule, this name cannot be changed.
12) Saving the NAT rule:
   - If you have configured a new NAT rule, click **Add** and then **OK**. The new NAT rule is inserted at the end of the table.
   - If you have edited an existing NAT rule, go to step 5.

13) Click on **Apply**. An activated NAT rule is identified under the menu item **NAT** with a green symbol.

20.1.2.3 How to Delete a NAT Rule

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Telephony** > **Routing**.
2) In the navigation tree, click **Routing**.
3) Click on **NAT** in the menu tree.
4) Click on the NAT rule to be deleted in the menu tree and click the **Delete NAT** tab. You cannot delete predefined default NAT rules.
5) Confirm the warning with **Delete** and then click **OK**. The NAT rule is deleted from the list of NAT rules under the **NAT** menu item.

20.1.3 Application Firewall

The Application Firewall is used to restrict access to specific services such as FTP or LDAP. It is disabled by default and can be enabled by defining appropriate rules.

The following services can either be blocked or restricted to specific IP addresses or IP address ranges by the Application Firewall in OpenScape Business X:

Service	Ports
FTP	21, 40000 - 40040
ssh (locked by default)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
OBSERVER	This service allowed access from an OpenScape Observer application, that is no longer supported.

Only the listed services can be blocked via a selection menu in Expert mode.

Telephone features such as SIP, HFA, etc. cannot be blocked using the Application Firewall.

A service can be selected multiple times; each time, different IP restrictions can be specified.

NOTICE: The activation/deactivation or modification of firewall parameters may severely restrict the functionality of the board (LAN-based administration may no longer be possible, for example).

NOTICE: The Application Firewall, when enabled, does not block services by default until a rule for that service is added, at which point only IP addresses included in the rule can access that specific service.

The Application Firewall may restrict access to inter-node features when the system is networked to other OpenScape Business systems. As an example the survivability feature requires the POSTGRES service to function correctly, in this case if a rule is added for the POSTGRES service manually add the IP addresses of the other OpenScape Business networked nodes to the POSTGRES rule to ensure correct operation of the survivability feature.

20.1.3.1 How to Display the Configuration of the Application Firewall

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **Application Firewall**.
4) Click on the **Display Services** tab to view the blocked services.
5) The name of the rule is displayed in the **Rule Name** field.
6) The check mark under **Rule activated** shows you whether or not a rule is enabled.
7) In the field **Lower Limit of Source IP Address Range** you will see the lower limit of the blocked IP addresses.
8) In the field **Upper Limit of Source IP Address Range** you will see the upper limit of the blocked IP addresses.

20.1.3.2 How to Restrict Services using the Application Firewall

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **Application Firewall**.

4) Click on the **Add Service** tab to block a range of IP addresses and/or a service.
5) Assign a name for this service (this rule) under **Rule Name**.
6) Under **Address Range**, enter the **Lower Limit** and the **Upper Limit** for the allowed source IP addresses.

   It is possible to block access completely by entering 127.0.0.1.

   INFO: You should activate a rule only after you are convinced that the authorized IP addresses have been configured correctly!

7) Click on **Save**.

20.1.3.3 How to Delete the Configuration of the Application Firewall

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **Application Firewall**.
4) Click on the **Delete all Services** tab to delete all services.

20.1.4 Services Administration (OpenScape Business S)

The Linux-internal firewall is enabled by default, which prevents access to OpenScape Business S. The communication system does, however, also provide services (e.g., the telephony service) that require open ports (services). After the installation of OpenScape Business S, these required ports/services must therefore be opened in the firewall. If services such as SNMP are not to be used, they can be disabled in the Linux firewall.

NOTICE: Note that the blocking of services that are used by OpenScape Business S can lead to a degradation and/or failure in the functionality of the communication system.

20.1.4.1 How to Add or Block Services

Step by Step

1) Click on **Computer** in the task bar.
2) In the menu tree, click on **System** > **YaST**.
3) Enter the password for the root user and click **Continue**.
4) Click on **Security and Users** in the menu tree.
5) In the **Security and Users** area, click on **Firewall**.

6) In the menu tree of the **Firewall Configuration: Start-up** window, click on **Allowed Services**.
7) In the field **Allowed Services for Selected Zone**, select the area for which you want to change services (**External Zone**, **Demilitarized Zone**, **Internal Zone**).
8) In the field **Service to allow**, select the specific services to be enabled (added) and click on **Add**. All currently permitted services are listed in the pull-down menu.
9) In the **Allowed Service** field, select the services to be disabled and click on **Delete**.
10) Enable the **Protect Firewall from Internal Zone** check box required.
11) Click on **Advanced** to add any ports or numeric protocols to the firewall (**TCP Ports**, **UDP Ports**, **RPC Ports** and **IP Protocols**). Click OK when finished.
12) Click on **Next** to display a window with your firewall settings. If required, you can view more information via **Show Details**.
13) Click on **Finish**.

20.2 Signaling and Payload Encryption (SPE)

SPE is a security feature for the transmission of signaling and payload data between IP system phones and the communication system. The feature is based on an asymmetrical encryption mechanism in which public and private keys are used.

Encryption of signaling and payload data:

- Signaling encryption: The signal transmission between the gateway and clients is encrypted with a 128-bit key. The TLS protocol with AES encryption is used for the transmission.
- Payload encryption: The payload or voice data is transmitted using the Secure Real-time Transport Protocol (SRTP). They are likewise encrypted with a 128-bit key (AES). SRTP is also used for IP networking. The procedure for exchanging the key for SRTP is known as Multimedia Internet Keying (MIKEY).

For SPE, the individual system telephones and communication systems involved must be able to uniquely identify one another. This is achieved through certificates, which also provide the public keys.

The keys and certificates are distributed by the DLS server; however, they can also be distributed manually.

INFO: The SPE feature is not offered for SIP and WL2 subscribers.

An encrypted connection only exists for direct connections between two system telephones or for conferences.

SRTCP Encryption

SRTCP (Secure Real-time Transport Control Protocol) is an extension of the SRTP protocol and implements the security of control data. The extension

consists of three additional fields: an SRTCP index, an encryption flag and an authentication tag.

SPE conformity

Family / Protocol / Interface	Signalling Encryption								Payload Encryption				
	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)		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

Legend:

Signaling encryption	
nv	No VoIP security
t	Default: TLS on the VoIP side; no end-to-end secure payload
s	Signaling and Payload Encryption (SPE)
*	No End-to-end Signaling Encryption (TLS)
Payload encryption	
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

20.2.1 How to Enable or Disable SPE Support

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **System Flags**.
4) Select one of the following options:
   - If you want to enable Signaling and Payload Encryption, select the **SPE Support** check box.
   - If you want to disable Signaling and Payload Encryption, clear the **SPE Support** check box.
5) Click on **Apply** followed by **OK**.

20.2.2 How Change the SPE Security Settings

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Security** > **Signaling and Payload Encryption (SPE)**.
3) In the **Edit Security Configuration** tab, under **Minimal length of RSA keys**, select the minimum key length for the security protocol (512, 1024 or 2048).
4) Select the item **Check certificate with CRL monitoring** if you want to a comparison with the CRL (certificate revocation lists) lists.
5) Under **Maximum Re-Keying interval [hours]**, enter the time (in hours) after which the key pairs are reassigned.
6) Click on **Apply**.

20.2.3 How to Import an SPE Certificate and Private Key (PKCS#12)

If no custom certificate is available, a self-signed CA certificate can be generated via SSL > Certificate Generation to produce and save a CA-signed server certificate (PKCS #12) that can be saved. This is then imported for SPE.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click on **Security** > **Signaling and Payload Encryption (SPE)**.
3) Navigate in the menu tree to **SPE Certificate**.
4) Enter the password for decryption that was created when generating the file under **Import SPE certificate plus private key (PKCS#12 file)** in the **Passphrase for decryption** field.
5) Under **File with certificate and private Key (PEM or PKCS#12 format)**, enter the name of the certificate file or click on **Browse** to search for it.

INFO: After you install a certificate for the first time with SPE enabled, an automatic reset is performed!

---

6) Click on **View Fingerprint of Certificate** to check the integrity of the certificate.

20.2.4 How to Import an SPE CA Certificate

This step is not required when using certificates that were created under **SSL Certificate Generation** itself.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Security** > **Signaling and Payload Encryption (SPE)**.
3) Navigate in the menu tree to **SPE CA Certificate(s**.
4) In the **Import trusted CA certificate (X.509 File) for SPE** window, under **File with certificate (PEM or binary)**, enter the file name of the certificate file or click **Browse** to select a file.
5) Under **CRL Distribution Point (CDP) Protocol**, select the protocol for the CRL (certificate revocation lists) lists (**LDAP** or **HTTP**).
6) Under **CDP (without ldap://, for example)**, enter the desired server.
7) Click on **View Fingerprint of Certificate**.

20.2.5 How to Enable or Disable SPE for a Station

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Navigate in the menu tree under **Stations** > **Station** > **IP Clients** down to the desired station (system client).
3) Navigate in the **Stations** window under the **Edit station parameters** tab to the **Payload Security** entry.

4) Select one of the following options:
   - If you want to activate the function, select the item **On** under **Payload Security**.
   - If you want to deactivate the function, select the item **Off** under **Payload Security**.
5) Click on **Apply**.

20.3 Virtual Private Network (VPN)

A virtual private network (VPN) is a PC network used to transport private data in a public network (such as the Internet). It therefore transfers data securely over an insecure network. Data is transmitted in encrypted format.

Overview of a VPN

VPN offers you:

- Secure connection via an unprotected medium (Internet)
- Protection of confidential data against manipulation
- Reliable integration of external partners in the corporate network
- Access to corporate information for field service

To ensure secure communications, VPN works as follows: A tunnel is created between the communication peers. In this instance, tunnel configuration is subject to authentication and authorization. The actual data is encrypted following tunnel configuration.

A VPN can be set up between (at least) two computers or networks (tunnel endpoints).

Two types of networking exist:

- Site-to-Site VPN

  This type of networking performs encryption between two VPN gateways; data is transferred unencrypted within the LANs.

- End-to-Site VPN

  Remote access VPN (remote access by mobile teleworkers)

System-Specific Information

The VPN parameters are principally administered via the VPN wizard.

Note that the connection to the communication system must be a secure SSL connection using OpenSwan or OpenSSL.

Dependencies

Topic	Dependency
DynDNS	The VPN endpoints must be reachable via a domain name or a fixed IP address. If this is not the case, DynDNS can be used.
DynDNS	If you change an IP address in VPN, the communication system updates the host-name-specific data (IP address) in DynDNS.

Topic	Dependency
DNS	Every VPN partner can resolve the host name/IP address via the standard DNS protocol. All DNS names (such as host name) must be fully qualified domain names (FQDN). Connections via IPSec tunnels are not possible while the IP address is being updated via DNS.

20.3.1 Requirements for VPN

To ensure the quality of the voice and data transmissions, the networks being used must satisfy certain requirements. Due to encryption, in particular, more bandwidth than for other networks must be planned.

In the following examples and in the tables, the encryption mode "ESP Tunnel Mode with Authentication" is used as a basis. This mode offers the highest security for site-to-site VPNs.

Structure of an encrypted voice packet:

Length of the ESP Header

Padding

Bandwidth calculation for the AES encryption algorithm:

Bandwidth calculation for the DES/3DES encryption algorithm:

Bandwidth for T.38 Fax

Protocol	Bytes	
ESP Trailer	12	
ESP Padding	varies (y)	encrypted
ESP Padding Header	2	encrypted
Voice Payload	varies (x)	encrypted
RTP	12	encrypted
UDP	8	encrypted
IP (original)	20	encrypted
ESP header	8 + iv	
IP (tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Total	**112 + iv + x + y**	

The length of the ESP header depends on the encryption algorithm used.

Required for Cipher Block Chaining. The ESP header contains an initialization vector (IV). The length of the IV is identical to the length of the cipher block.

Padding is required, since the encryption algorithm is based on cipher block chaining. This means that the entire encrypted portion of the packet (original IP/ UDP/ RTP header + voice payload+ESP header padding) must correspond to an integral multiple of the cipher block length.

Block length of the encryption algorithm:

Encryption Algorithm	Block length	Length of the initialization vector
AES	16 bytes (128 bit)	16 bytes (128 bit)
3DES	8 bytes (64 bit)	8 bytes (64 bit)

Calculation of the required padding bytes for voice packets:

(42 + x + y) (bytes) = N x (0 or 16 (bytes)) (N integer)

Codec	Packet parameters	Frame size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	294	75%	117.6
G.711	30	30	240	6	372	50%	99.2
G.711	40	40	320	6	454	38%	90.8
G.711	60	60	480	6	614	25%	81.9
G.729A	1	20	20	2	150	600%	60.0
G.729A	2	40	40	6	182	300%	36.4
G.729A	3	60	60	2	198	200%	26.4

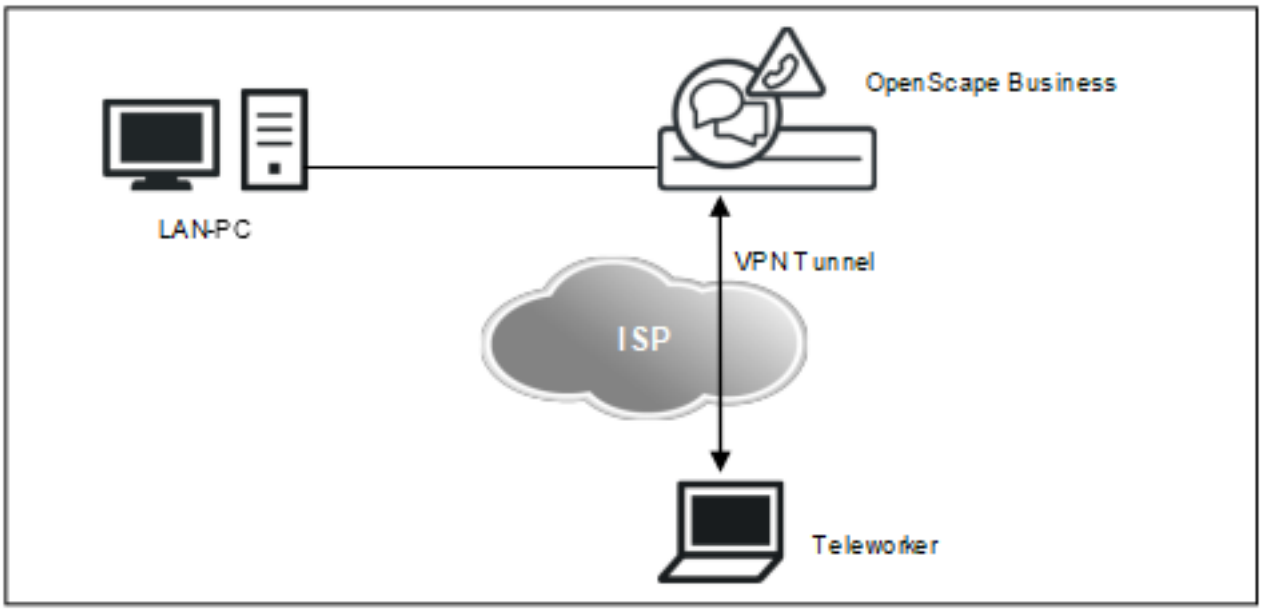
Codec	Packet parameters	Frame size (ms)	Payload (bytes)	Padding (Bytes)	Ethernet packet length (bytes)	Payload / Packet overhead ration	Ethernet load (incl.) header (kbps)
G.711	20	20	160	6	286	75%	114.4
G.711	30	30	240	6	366	50%	97.6
G.711	40	40	320	6	446	38%	89.2
G.711	60	60	480	6	606	25%	80.8
G.729A	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

Encryption Algorithm	Frame size (ms)	Payload y (bytes)	Padding x (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl.) header (kbps)
DES / 3DES	30	169	1	278	64%	74.1
AES	30	169	9	294	74%	78.3

20.3.2 Connecting Teleworkers via a VPN

Teleworkers can be connected to the communication system via a secure VPN connection.

Stand-alone System with Integration of Teleworkers via a VPN



The communication system provides integrated VPN functionality (configured using a wizard). Per communication system, up to 10 teleworkers can be simultaneously active via a VPN connection.

The following VPN clients have been released for OpenScape Business:

- NCP VPN Client
- Shrew Soft VPN Client
- Android VPN Client
- iOS VPN Client
- Mac OS-X VPN Client

Exporting the Teleworker Data

The teleworker data can be exported as a ZIP file (unencrypted). For each supported VPN client, the ZIP file contains a separate text file with the teleworker data. This is an `.ini` file for the NCP VPN client, a `.vpn` file for the Shrew Soft VPN Client and a `.networkConnect` file for the OS X VPN client. These text files can be imported at the VPN client.

INFO: Umlauts or accents in the text files with the teleworker data are ignored. Blanks are replaced by underscores.

Status Display of VPN Connections

A status display of all VPN connections can be found in the **VPN** wizard. A detailed overview of all VPN connections can be found in the **Service Center** under **Diagnostics** > **Status** > **VPN Status**.

VPN with OpenScape Business S

With OpenScape Business S, the VPN is terminated via an external router. The description of external applications is not part of this documentation.

20.3.2.1 How to Connect Teleworkers via a VPN

The **VPN** wizard can be used to grant VPN teleworkers (VPN partners) access to the internal LAN and to connect communication systems via a VPN (virtual private network). If the communication system does not have any fixed external IP address (public IP address, global IP address), a DynDNS service will need to be configured (at www.dyndns.org, for example).

Prerequisites

Internet access via the WAN interface has been configured.

If the WAN interface has no fixed (public) IP address, DynDNS must be configured. A connection to the Internet is required for a successful DynDNS test.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.
4) Click **Configuration of VPN**.
5) If you want to edit a configured VPN connection, click on **Edit** for the desired VPN connection.
6) If you want to create a new VPN connection, click on **Add**.
7) Enter a name for the VPN connection (e.g., `node2mch.dyndns.org`) in the **System name** field.
8) If desired, enter a **Comment** in the corresponding field.
9) Select the **enabled** check box (already preset by default).
10) Select the check box **Use Data of own System**.
11) If required, select the **Address Type**:
    - If the WAN interface has a fixed (public) IP address, select the entry **IP Address** from the **Address Type** drop-down list and enter the fixed (public) IP address under **Global Address / DNS Name (WAN)**.
    - If the WAN interface does not have a fixed (public) IP address, select the entry **DNS Name** from the **Address Type** drop-down list. The DNS name of the communication system that is already configured for DynDNS will be displayed under **Global Address / DNS Name (WAN)**.
12) The **Local IP Address (LAN)** should only be changed if required.
13) The **Local Subnet Mask (LAN)** should only be changed if required.
14) If you want to edit one of the already configured teleworkers, click on **Edit** next to the desired teleworker in the **Teleworkers** area.
15) If you want to create a new teleworker, click on **Add** in the **Teleworkers** area.

16) Enter a teleworker configuration name in the **Name** field.
17) Configure the type of the VPN client being used:
    - For pure IPSec VPN teleworkers (NCP and Shrew Soft VPN Clients):

      Clear the **L2TP/IPSec** check box and select the **IP Address** as **Address Type**. Enter a virtual IP address / DynDNS name for the teleworker in the field **Virtual IP address/DynDNS Name** if the VPN client being used supports virtual IP addresses (regardless of whether the teleworker has an Internet connection via a DSL router or DSL modem).
    - For L2TP/IPSec VPN teleworkers (iOS, Android and MAC OS X VPN clients):

      Select the **L2TP/IPSec** check box and assign a **User name** and a **Password** to the teleworker.
18) Select the **enabled** check box (already preset by default).
19) Click **OK**. The window with the overview of teleworkers is displayed again. You can enter further teleworkers.
20) When you have set up all teleworkers, click **OK & Next**. The **System Selection** window is displayed.
21) Click **OK & Next**. The **Security setup for connections** window appears.
22) To ensure a secure VPN connection, assign a key for the newly configured VPN connection under **PreShared Secret** and repeat it under **Repetition of the PreShared Secret**. The key must be at least 20 characters in length.
23) Enter a **Comment** if required.
24) Click **OK**. The **VPN Status Information** window appears.
25) Click on **Switch VPN on**.
26) Only if the address type DNS Name has been selected: Check the already configured data of the DynDNS account and click on **Connection test**. The DNS access data is now transmitted to the service provider. This procedure takes approximately 10 seconds. If the test is not successful, check your access data. After the test succeeds, click **OK**.
27) Click **OK & Next**. The teleworkers can now access the WAN interface of the communication system.
28) Click **Finish**.

20.3.2.2 How to Export Teleworker Data

You can export the teleworker data with the **VPN** wizard.

Prerequisites

A VPN connection is configured.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.

4) Click on **Export/Import**.
5) Click on **Export** in the **Export Teleworker Data from System** area. Save the ZIP file to a location of your choice.

> **INFO:** For each supported VPN client, the ZIP file contains a separate file with the teleworker data. The teleworker data is not encrypted! Please take a responsible approach to the data.

6) Click **OK & Next** followed by **Finish**.

20.3.3 Networking Communication Systems via a VPN

Several OpenScape Business communication systems can be networked together securely using a site-to-site VPN network.

Networking via VPN

You can optionally configure all the data required for networking multiple systems on one communication system, encrypt and export this topology data and then import it on all other systems. This enables a fast and consistent configuration on all systems in the internetwork.

The distinction between the own system and the foreign systems occurs through the detection of the own DynDNS name or (when using fixed IP addresses) through the own Internet address.

- Exporting topology data from a system
  - All data about the topology of the VPN network is written to an encrypted XML file and provided as a ZIP export file for import into another system.
- Importing topology data into a system
  - All data about the topology of the VPN network can be imported from the ZIP file (with the encrypted XML file) and applied to this system.

The key (password) for export is freely selectable and must be communicated to any other administrator who may want to import these settings.

Status Display of VPN Connections

A status display of all VPN connections can be found in the **VPN** wizard. A detailed overview of all VPN connections can be found in the **Service Center** under **Diagnostics** > **Status** > **VPN Status**.

20.3.3.1 How to Configure Networking via a VPN

The **VPN** wizard can be used to configure all communication systems which are connected to a system via VPN. This topology data can be exported and imported into all systems in the VPN internetwork.

Prerequisites

Internet access via the WAN interface has been configured.

If the WAN interface has no fixed (public) IP address, DynDNS must be configured. A connection to the Internet is required for a successful DynDNS test.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.
4) Click **Configuration of VPN**.
5) Click **Add**.
6) Enter a name for the first system in the VPN internetwork (e.g., `node1mch.dyndns.org`) in the **System name** field.
7) If desired, enter a **Comment** in the corresponding field.
8) Select the **enabled** check box (already preset by default).
9) Select the check box **Use Data of own System**. The following fields are automatically populated with the system data.
10) The preset **Address Type** should only be selected if required:
    - If the WAN interface has a fixed (public) IP address, select the entry **IP Address** from the **Address Type** drop-down list and enter the fixed (public) IP address under **Global Address / DNS Name (WAN)**.
    - If the WAN interface does not have a fixed (public) IP address, select the entry **DNS Name** from the **Address Type** drop-down list. The DNS name of the communication system that is already configured for DynDNS will be displayed under **Global Address / DNS Name (WAN)**.
11) The preset **Local IP Address (LAN)** should only be changed if required.
12) The preset **Local Subnet Mask (LAN)** should only be changed if required.
13) Click **OK & Next**. The **System Selection** window is displayed.
14) Click again on **Add**.
15) Enter a name for the second system in the VPN internetwork (e.g., `node2mch.dyndns.org`) in the **System name** field.
16) If desired, enter a **Comment** in the corresponding field.
17) Select the **enabled** check box (already preset by default).
18) Select the **Address Type** for the second system:
    - If the WAN interface has a fixed (public) IP address, select the entry **IP Address** from the **Address Type** drop-down list and enter the fixed (public) IP address under **Global Address / DNS Name (WAN)**.
    - If the WAN interface does not have a fixed (public) IP address, select the entry **DNS Name** from the **Address Type** drop-down list. The DNS name of the communication system that is already configured for DynDNS will be displayed under **Global Address / DNS Name (WAN)**.
19) Enter the **Local IP Address (LAN)** of the second system.
20) Enter the **Local Subnet Mask (LAN)** of the second system.
21) Click **OK & Next**. The **System Selection** window is displayed.
22) Repeat steps 14 through 21 for other systems in the VPN internetwork.
23) Then click **OK & Next**. The **Security setup for connections** window appears.

24) Assign a separate key for each VPN connection between systems under **PreShared Secret** and repeat it under **Repetition of the PreShared Secret**. The key must be at least 20 characters in length.
25) Enter a **Comment** for each VPN connection if required.
26) Click **OK**. The **VPN Status Information** window appears.
27) Click on **Export/Import** to export the topology data. The **Export and Import of VPN Configuration Data** window appears.
28) In the **Export Topology Data from System** area, specify a key (at least 7 digits) for backing up the data under **Key** and **Repeat Key** and then click on **Export**. Save the file to a location of your choice.
29) Click **OK & Next**.
30) Click on **Switch VPN on**.
31) Only if the address type **DNS Name** has been selected: Check the already configured data of the DynDNS account and click on **Connection test**. The DNS access data is now transmitted to the service provider. This procedure takes approximately 10 seconds. If the test is not successful, check your access data. After the test succeeds, click **OK**.
32) Click **OK & Next** followed by **Finish**.
33) In the WBM of the second system, click on **Setup** in the navigation bar and on **Wizards** > **Network / Internet** in the navigation tree.
34) Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.
35) Click on **Export/Import** to import the topology data. The **Export and Import of VPN Configuration Data** window appears.
36) Click on **Import Topology Data to System** to import the topology data into the system.
37) Enter the **Key** (password) you used when exporting the data from the first system.
38) Navigate to the storage location of the ZIP file. Then click on **Import**.
39) Click **OK & Next**. You can see the configured systems.
40) Click on **Switch VPN on**.
41) Only if the address type **DNS Name** has been selected: Check the already configured data of the DynDNS account and click on **Connection test**. The DNS access data is now transmitted to the service provider. This procedure takes approximately 10 seconds. If the test is not successful, check your access data. After the test succeeds, click **OK**.
42) Click **OK & Next** followed by **Finish**.
43) Repeat steps 33 through 42 for the remaining systems in the VPN internetwork.

20.3.3.2 How to Import and Export the Topology Data of a VPN Network

The **VPN** wizard can be used to export and import the topology data of the VPN network.

Prerequisites

A VPN connection is configured.

In order to import the topology data, you will need to know the key that was assigned when exporting that data.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Network / Internet**.
3) Click **Edit** to start the **VPN Configuration** wizard. The default setting is **VPN is switched off**.
4) Click on **Export/Import**.
5) If you want to export the topology data, in the **Export Topology Data from System** area, specify a key (at least 7 digits) for backing up the data under **Key** and **Repeat Key** and then click on **Export**. Save the file to a location of your choice.
6) If you want to import the topology data, in the **Import Topology Data to System** area, enter the key to decrypt the data under **Key** and then navigate to the storage location of the ZIP file. Then click on **Import**.
7) Click **OK & Next** followed by **Finish**.

20.3.4 VPN - Security Mechanisms

In VPN, the encryption of data occurs via different security mechanisms such as IPSec tunneling, Security Associations and authentication methods (peer-to-peer, digital signatures).

IPSec Tunnels

IPSec is used to encrypt data and can generally be implemented with and without tunnels. IPSec is an option for implementing VPN. You can encrypt the entire IP packet here with the IP header: this occurs in tunnel mode.

Tunnels must always be configured for both VPN peers.

IPSec supports the automatic key management system, Internet Key Exchange (IKE). This is a standard that is integrated in IPSec.

Security Associations SA

IKE SA

Payload SA

Authentication

A security association (SA) is an agreement between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

VPN connections always require three security associations (SA), negotiated in two phases:

- Phase 1 - Generating the IKE SA

  One for the initial mutual authentication and for exchanging the session keys (IKE-SA)

- Phase 2 - Negotiating the payload SAs

  One for each direction in the connection for payload traffic once established (payload SAs)

The IKE protocol has essentially two different tasks. Start by creating a protocol used exclusively by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data. IKE therefore operates in the two consecutive phases:

When setting up a call between VPN partners, various parameters must be negotiated (such as how often a key is regenerated or which encryption procedures are used). These parameters are stored and administered in IKE SAs.

IKE phase 2 is used to negotiate all security parameters for the payload SAs between the VPN partners.

You always have to configure two SAs for transmission and receipt.

The following steps are essentially performed:

- Negotiating the algorithms for encryption and authentication
- Negotiating the security protocols used (ESP and AH)
- Negotiating the security protocol operating mode
- Negotiating the SA lifetime
- Defining the key material

Peer-to-peer communication in VPN. The following two types of authentication are possible for VPN peers:

- Pre-shared keys

  Pre-shared keys are also mostly used for VPN. A key pair is configured for both VPN partners for this. These keys form a "hash value" which is verified by the relevant partners for authentication purposes.
- Digital signatures

  Every VPN partner is assigned a certificate. For successful authentication, the VPN peers at both tunnel endpoints must check the digital signature of their peer against a trusted CA.

System-Specific Information

The VPN parameters are principally administered via the wizard.

Note that the administrator connection must run via a secure connection with SSL.

- Security Associations SA

  The communication system supports Oakley groups 1, 2, and 5.
- IPSec

  The communication system uses IPSec tunnel mode with ESP (Encapsulating Security Payload). ESP is an IPSec protocol that guarantees packet encryption, packet integrity as well as packet authenticity

- Payload SA

  The communication system supports the encryption algorithms DES, 3DES, and AES

  Of all the MAC algorithms (MAC=Message Authentication Code) for authenticating data origin and data integrity, HMAC-SHA1, HMAC-SHA2, and HMAC-MD5 are supported.
- Recommended operating modes
  - IKE in "Main Mode" with Perfect Forward Secrecy
  - Hash function with SHA-2
  - Authentication with certificates (RSA)
  - Encryption with AES (up to 256 bits)
  - Support for dynamic public IP addresses via virtual IP addresses or DynDNS updating mechanisms for teleworker PCs

20.3.5 VPN - Certificates

A certificate binds a specific public key to a specific VPN client. In this case, the client can be both a client of the communication system and a teleworker. The unique combination of public key and VPN client provides the basis for authentication.

Certificates and certificate authority

Lightweight CA

Certificate revocation lists (CRL)

Certificates are digitally signed and generated by a certificate authority (CA). IPSec accepts a certificate if it is issued by a trusted certificate authority.

In a simple VPN environment, the definition of an individual certificate authority may be sufficient; this CA operates as a trusted master certificate authority for the entire VPN and uses its self-signed CA certification for identification at all VPN clients.

Every VPN client needs one of the certificates issued by this CA.

Certificates based on the X.509 standard (the most widely used standard today) include the following main elements:

- information about the identity of the certificate owner
- the public key of the certificate owner,
- information about the CA that signed the certificate (a serial number, the validity period, information about the identity of the CA, and the digital signature of the CA)

A Lightweight CA function helps with certification in environments where the customer is not already using a PKI. A Lightweight CA offers the following options:

- creating public/private key pairs
- signing and generating corresponding certificates
- saving key pairs with associated certificates in files

In cryptographic terms, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates.

A critical situation occurs when a certificate has become known (or if this is suspected), and this certificate is hence no longer trustworthy for the peer authentication. In this case, the certificate authority must revoke the certificate and the revocation must be signaled to all peers as soon as possible. A remote peer's attempt to authenticate its identity using a revoked certificate is denied.

Basically, a CRL is a list of all revoked certificates. CRLs always have to be generated by the CA where the certificates originate.

A CRL contains the following main elements:

- a list of all revoked certificates; the certificates are identified by serial numbers
- the publication date for the next CRL updated (specifies the time to live for the CRL)
- information about the CA that generated the certificate (information on the identity of the CA and the digital signature of the CA)

The administrator must manually update and distribute the CRLs at regular intervals.

System-Specific Information

Authentication is performed on the basis of cryptographic algorithms with public keys. The communication system supports RSA as the algorithm for cryptography with public keys. The communication system only supports certificates that correspond to the X.509 standard.

The communication system always operates as a VPN client for authentication.

- Lightweight CA

  The communication system offers restricted CA functionality (Lightweight CA). The administrator provides the key material for a system by manually importing private/public key pairs and certificates via the SSL-secured administration connection for all communication partners involved.

- CRL

  CRLs (certificate revocation lists) are used to revoke certificates. The CRL is imported into the communication system by the administrator via an SSL-protected connection.

20.3.5.1 VPN - How to Generate Lightweight CA Certificates

Lightweight CA is a licensed function for generating and managing CA and peer certificates.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **Security**.

3) Navigate in the menu tree to **VPN** > **Lightweight CA**. You can generate a CA certificate of your own in the **Generate Certificate** window.

4) Enter a name for the requested certificate under **Certificate Name**.

5) Enter a serial number of your choice under **Serial Number of the Certificate**

INFO: A serial number that has already been assigned cannot be used again for another certificate, since the serial numbers for all certificates that were ever created must be unique.

---

6) Under **Type of Signature Algorithm**, enter the desired algorithm for the certificate (sha256RSA or sha512RSA).
7) Under **Public Key Length**, enter the length of the public key (e.g., 2048).
8) Enter the date and time for the start of the validity period under **Start Time of Validity Period (GMT)**. The date specified is interpreted as Greenwich Mean Time (GMT).
9) Enter the date and time for the end of the validity period under **End Time of Validity Period (GMT)**.
10) Under **Subject Name**, enter the **Country (C)**, the **Organization (O)**, the **Organization Unit (OU)** and **Common Name (CN)**.
11) You can optionally also enter an alternative subject name under the **Subject Alternative Name** field. If you have done this, you will also need to select a format (e.g., IP address or DNS name). The input window depends on the selected format.
12) Enter the distribution point for the CRL lists (listed in a drop-down menu) in the **CRL Distribution Point** field.
13) Click on **Generate Certificate**.

20.3.5.2 VPN - Certificate Management - How to View a Certificate

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Certificate Management**. The **View Certificate From File** window appears.
4) Activate the **PKCS#12 Format** check box if required.
5) Enter the **Passphrase for decryption**.
6) Enter the certificate file under **File with Certificate** or select it using **Browse**.
7) Click on **Load**.

20.3.5.3 VPN - How to Import a Trusted CA Certificate (X.509)

X.509 is a standard for certificates. In this case, the name and digital signature of the issuer of the certificate are also saved in the certificate. X.509 is part of the X.500 directory service for world-wide, distributed, and open systems.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Certificate Management** > **Trusted CA Certificates** > **Configured Certificates**.
4) Enter a name for the requested certificate under **Certificate Name**.
5) Enter the certificate file under **File with Certificate** field or select a certificate file using **Browse**.
6) Confirm and click on **Activate the Configured VPN Tables.**

20.3.5.4 VPN - Peer Certificates - How to Generate a Certificate Signing Request (CSR)

You can generate a CA-signed peer certificate based on a CA certificate. This requires at least one CA certificate to have already been generated. The certificate generated is saved in a PKCS#12 file. PKCS#12 files (Personal Information Exchange Syntax Standard) save certificates with the private key. A PKCS#12 file therefore contains the necessary data for personal encryption and decryption.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Peer Certificates**.
4) Enter the required data on the **Generate Certificate Signing Request (CSR)** tab.
5) Enter the **Certificate Request Name**.
6) Enter the desired algorithm (sha256RSA or sha512RSA) under **Type of Signature Algorithm**.
7) Enter the key length (2048) under **Key Length**.
8) Under **Subject Name** enter all the relevant data for **Country (C)**, **Organization (O)**, **Organization Unit (OU)** and **Common Name (CN)**.
9) Under **Subject Alternative Name**, enter the **Distinguished Name Format**, any possible **Other Format** or an **Alternative Subject Name**.
10) Save the *.csr file to be signed by a CA.

20.3.5.5 VPN - Peer Certificates - How to Generate a Certificate (PKCS#12)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Lightweight CA**.
4) Click on the CA certificate and then on **Generate CA-Signed Peer Certificate [PKCS#12]**.
5) Enter the **Passphrase for decryption**.
6) Enter a serial number of your choice under **Serial Number of Certificate**.
7) Enter the key length (1024, 1536 or 2048) under **Key Length**.
8) Enter the date and time for the start of the validity period under **Start Time of Validity Period (GMT)**. The specified date and time is in Greenwich Mean Time.

   NOTICE: The validity period of the peer certificate must be carefully adapted to comply with the applicable security guidelines in the company. Shortly before the validity period expires, the certificate must be extended or a new certificate must be issued.

9) Enter the date and time for the end of the validity period under **End Time of Validity Period (GMT)**.
10) Under **Subject Name** enter all the relevant data for **Country (C)**, **Organization (O)**, **Organization Unit (OU)** and **Common Name (CN)**.
11) You can optionally also enter an alternative subject name under the **Subject Alternative Name** field. If you have done this, you will also need to select a format (e.g., IP address or DNS name). The input window depends on the selected format.
12) Enter the **CRL Distribution Point** (optional).
13) Click on **Generate Certificate**.

20.3.5.6 VPN - How to Import a Peer Certificate (PKCS#12)

PKCS#12 files (Personal Information Exchange Syntax Standard) save certificates with the private key. A PKCS#12 file thus contains the essential data for personal encryption and decryption.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Peer Certificates**.
4) Click on the **Import Peer Certificate (PKCS#12)** tab.
5) Enter a name for the requested certificate under **Name of the Certificate**.
6) Under **Passphrase for decryption**, enter your personal password for decrypting this certificate.

7) Enter the file name under **File with Certificate** or locate the file by using the **Browse** button.
8) Click on **View Fingerprint of Certificate**.
9) Click on **Import Certificate from File**.

20.3.6 VPN Clients

Teleworkers can establish a secure VPN connection to the corporate network using a VPN tunnel over the Internet. To do this, a VPN client must be installed on their device (PC, tablet PC, smartphone). All data transmitted between the VPN client, the corporate firewall and the VPN server of the communication system is encrypted.

The following VPN clients are supported:

- **NCP VPN Client**

  NCP clients can be used in any VPN environments with IPSec. This is significant if access is required from a remote PC to VPN gateways of different manufacturers or if a central VPN gateway from a third-party vendor is already installed in the company network. In the case of a branch office network, the NCP Secure Enterprise Gateway can be used with other VPN gateways on the basis of IPSec connections.

  The NCP client is not free, but it offers the benefits of a graphical user interface and a status indicator for the connection.
- **Shrew Soft VPN Client**

  The Shrew Soft VPN Client is a free VPN client with a graphical user interface that supports version 2.1.5 and hybrid authentication.

  The Shrew Soft VPN client includes, among other things, ISAKMP, Xauth and RSA support, AES, Blowfish and 3DES encryption protocols, and numerous other features that are usually found only in professional solutions.
- **iOS and Android VPN Client**

  The L2TP/IPSec VPN client is integrated in the iOS or Android operating system.

  The L2TP/IPSec VPN clients use the IP address range `10.254.253.x`. If IP addresses from this range are already being used in the customer network, the IP address range needs to be changed in the WBM (e.g., from `10.254.253.1` to `10.254.252.1`) via **Expert mode** > **Maintenance** > **Application Diagnostics** > **IPSec Test: IPSec Test Routines** > **Set IP Address for L2TP**.
- **Mac OS-X VPN Client**

  The Mac OS X VPN client is integrated in the MAC OS X operating system.

System-Specific Information

- The teleworker data of a VPN client can be exported as a ZIP file (unencrypted). For each supported VPN client, the ZIP file contains a separate text file with the teleworker data. This is an `.ini` file for the NCP VPN client, a `.vpn` file for the Shrew Soft VPN Client and a `.networkConnect` file for the OS X VPN client. These text files can be imported at the VPN client.

- LAN infrastructure with multiple subnets

  If VPN is to be used for a LAN infrastructure with multiple subnets, it is necessary to create rules for these subnets. These rules cannot be created via wizards, but must be configured in Expert mode.
- Tunnel in Tunnel

  It is not possible create a second VPN tunnel through an already existing VPN tunnel.

20.3.6.1 NCP VPN Client Settings

VPN connections via the NCP VPN client require the following settings if the configuration is to be performed manually. You can export a text file with the configured VPN client data (`ncp_vpn.ini`) from your communication system and import it into the VPN client. This ensures that the respective configuration settings are populated automatically.

Basic Settings

- Profile name

  freely selectable; use of meaningful names recommended
- Connection type

  VPN to IPSec peer
- Connection medium

  In accordance with the Internet connection used

  e.g., LAN (over IP) or xDSL (PPPoE)

Dialing into network

No configuration required.

HTTP Login

No configuration required.

Modem

No configuration required.

Line Management

- Call setup

  automatic or manual

  Timeout = 0

  NOTICE: This ensures the connection is not cleared due to idle time!
- Prioritizing Voice over IP (VoIP)

  Set check mark
- EAP Authentication

  No configuration required

- HTTP authentication

  No configuration required

IPSec Settings

- Gateway = IP address or DNS name of the communication system

  The communication system can be reached via the Internet under this IP address or DNS name.

  Designation in the VPN wizard: **IP Address/DynDNS Name**
- IKE Policy = Unattended Mode
- IPSec Policy = Unattended Mode
- Exchange Mode = Main Mode
- PFS Group = DH Group 2 (1024 bits)
- Validity / Duration
  - IKE Policy: 000:00:07:00 (7 minutes)
  - IPSec Policy: 000:00:08:00 (8 minutes)
- Editor

  No configuration required

Advanced IPSec Options

No configuration required

Identity

- Type = IP address

  ID = IP address of the teleworker PC (see also: Assigning IP addresses)

  Use Pre-shared key

  Set check mark

  Shared Secret = This is the password for the VPN connection

  Designation in the VPN wizard: **PreShared Secret**
- Extended Authentication (XAUTH)

  not used, no configuration required

IP address assignment

- Assign IP address manually

  IP address = IP address of the teleworker PC

  Designation in the VPN wizard: **IP Address/DynDNS Name**
- DNS / WINS

  Set check mark
- DNS server = IP address of the communication system

  Designation in the VPN wizard: **Local IP Subnet Address (LAN)**

VPN - IP Networks

No configuration required.

Certificate check

No configuration required

Link Firewall

- Activate Stateful Inspection:

  for existing connection
- Allow only communication in the tunnel:

  Set check mark

20.3.6.2 How to Configure an NCP VPN Client

An NCP VPN client must be installed and configured on the teleworker device for a secure VPN connection to the communication system.

Prerequisites

The administrator of your communication system has set you up as a teleworker in the WBM of OpenScape Business and made the export ZIP file with the teleworker data available to you.

The administrator of your communication system has communicated the PreShared Secret Key for the VPN connection to you.

The NCP VPN client (LANCOM Advanced VPN Client) is installed on the teleworker device. The information required for this can be found in the documentation of the NCP VPN client.

The teleworker device has an existing and active connection to the Internet.

Step by Step

1) Extract the files `ncp_readme.txt` and `ncp_vpn.ini` and place them in a local directory. The entries in the `ncp_vpn.ini` file refer to the `HOOME` profile.
2) Import the `HOOME` profile into the NCP VPN client.
3) Extend the `HOOME` profile with a DNS server. The address of the DNS server is the private IP address (LAN) of your communication system.
4) Start the NCP VPN client
5) Select the `HOOME` profile and click on **Connect**.

20.3.6.3 How to Configure a Shrew Soft VPN Client

A Shrew Soft VPN Client must be installed and configured on the teleworker device for a secure VPN connection to the communication system.

Prerequisites

The administrator of your communication system has set you up as a teleworker in the WBM of OpenScape Business and made the export ZIP file with the teleworker data available to you.

The administrator of your communication system has communicated the PreShared Secret Key for the VPN connection to you.

The Shrew Soft VPN Client is installed on the teleworker device. A download for the Shrew Soft VPN client can be found under `http://www.shrew.net`.

The teleworker device has an existing and active Internet connection.

Step by Step

1) Extract the files `shrewsoft_readme.txt` and `shrewsoft_openswan.vpn` and place them in a local directory.
2) Start the **Shrew Soft VPN Client Access Manager** and configure it. Save the entries.
3) Import the file `shrewsoft_openswan.vpn` into the Shrew Soft client.
4) You should then see the connection in the **Shrew Soft Client VPN Access Manager** under **Connect**.

20.3.6.4 How to Configure an iOS or Android VPN Client

An L2TP VPN connection must be configured on the teleworker device for a secure VPN connection to the communication system.

Prerequisites

The administrator of your communication system has configured you as a teleworker in the WBM of OpenScape Business and has communicated the user name, the password and the PreShared secret key for the VPN connection to you.

The teleworker device has an existing and active connection to the Internet.

Step by Step

1) Open the **Settings** > **General** > **VPN** menu on the iOS or Android teleworker device.
2) Click on **Add VPN** to add a new VPN connection.
3) Click on the **L2TP** tab.
4) Enter a name for the VPN connection in the **Description** field.
5) Enter the public IP address or the DNS name of the communication system in the **Server** field.
6) Enter the teleworker user name in the **Account** field.
7) Enter the teleworker password in the **Password** field.
8) Enter the PreShared secret key for the VPN tunnel in the **Shared Secret** field.
9) Enable the **For all data** option.
10) Select the **VPN** option in the **Settings** menu.

20.3.6.5 How to Configure a Mac OS X VPN Client

An L2TP VPN connection must be configured on the teleworker device for a secure VPN connection to the communication system.

Prerequisites

The administrator of your communication system has set you up as a teleworker in the WBM of OpenScape Business and made the export ZIP file with the teleworker data available to you.

The administrator of your communication system has communicated the user name, the password and the PreShared secret key for the VPN connection to you.

The teleworker device has an existing and active connection to the Internet.

Step by Step

1) Extract the file `.networkConnect` and place it in a local directory.
2) Double-click on the file `.networkConnect`.
3) Click on **VPN (L2TP)**.
4) Select the VPN connection in the **Configuration** field.
5) Enter the public IP address or the DNS name of the communication system in the **Server Address** field.
6) Enter the teleworker user name in the **User Name** field.
7) Set the security settings:
   a) Click **Authentication Settings**.
   b) Enter the teleworker password in the **Password** field.
   c) Enter the PreShared secret key for the VPN tunnel in the **("Shared Secret") Key** field.
   d) Click **OK**.
8) Click on **More Options** and select the **Send all traffic over VPN connection** check box. Then click **OK**.
9) Click on **Apply**, followed by **Connect**. Once the connection to the OpenScape Business has been established successfully, the connection status will be shown as **Connected**.

20.3.7 VPN Services

You can manage services via the Configured Services function. Configured services become active services only on activation.

20.3.7.1 VPN - Active Services - How to Display all IPsec Services

A list of all active IPsec services with detailed information can be displayed in the form of a table.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Active Services**.

4) You can view the relevant details for the active IPSec services under the **Display IPsec Services** tab.

20.3.7.2 VPN - Active Services - How to Display a Special IPsec Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Active Services**.
4) Click in the menu tree on the special service for which you want to view all the information (**Name of the Service**, **Source Port**, **Destination Port**, **IP Protocol**, **Associated 'pass' Rule**, **Associated 'deny' Rule**).

20.3.7.3 VPN - Configured Services - How to Display all IPsec Services

A list of all configured IPsec services with detailed information can be displayed in the form of a table.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Configured Services**.
4) You can view the relevant details for the configured IPSec services under the **Display IPsec Services** tab.

20.3.7.4 VPN - Configured Services - How to Edit the IPsec Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

NOTICE: Before editing and/or enabling the IPSec service, a backup should be performed. IPSec rules behave like firewall entries and can restrict access to the system. If a situation arises in which you have enabled IPSec and can then no longer access the system, you can reset the communication system with **Reload**.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Configured Services**.
4) Click on the special service that you want to edit in the menu tree.
5) Edit the name of the service under **Name of the Service**.
6) Change the source port under **Source Port**.
7) Change the destination port under **Destination Port**.
8) Change the service (e.g., UDP) under **IP Protocol** den Service.
9) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.7.5 VPN - Configured Services - How to Rename the IPsec Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Configured Services**.
4) Click on the special service that you want to rename in the menu tree.
5) Edit the name of the service under **Name of the Service**.
6) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.7.6 VPN - Configured Services - How to Delete the IPsec Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Services** > **Configured Services**.
4) Click on the special service that you want to delete in the menu tree.
5) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.8 VPN tunnel

Tunnel is the term used to describe the transportation of encrypted data packets to a defined endpoint. Active tunnels become configured tunnels when the configuration is enabled. A maximum of 256 tunnels can be set up per gateway.

20.3.8.1 VPN - Active Tunnels - How to Display General Tunnel Data

You can view all active tunnels in tabular form with detailed information on them.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Tunnels** > **Active Tunnels**.
4) Under the **Display General Tunnel Data** tab you can view detailed information on each active tunnel. This includes:
   - **Name of the Tunnel**
   - **State in IP Stack**
   - **Endpoint type of the local tunnel**
   - **Local Tunnel Endpoint Address**
   - **Type of the Remote Tunnel Endpoint**
   - **Remote Tunnel Endpoint Address**
   - **Suggested Lifetime of the Session Keys**
   - **Suggested Lifetime of the Key Exchange Session**
   - **Associated Rules: Associated Transmit Rule**
   - **Associated Rules: Associated Receive Rule**

20.3.8.2 VPN - Active Tunnels - How to Display Rules for all Tunnels

You can have the rules for all active tunnels displayed in a window.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Tunnels** > **Active Tunnels**.
4) On the **Display Rules for all Tunnels** tab, you will see detailed information on each active tunnel such as
   - **Tunnel Data**
   - **Rule Data**
   - **Source Address**
   - **Destination Address**
   - **Service Data**

20.3.8.3 VPN - Configured Tunnels - How to Display General Tunnel Data

You can view all the data for configured tunnels in tabular form with detailed information on them.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Tunnels** > **Configured Tunnels**.
4) Under the **Display General Tunnel Data** tab you can view detailed information on each configured tunnel. This includes:
   - **Name of the Tunnel**
   - **Endpoint type of the local tunnel**
   - **Local Tunnel Endpoint Address**
   - **Type of the Remote Tunnel Endpoint**
   - **Remote Tunnel Endpoint Address**
   - **Suggested Lifetime of the Session Keys**
   - **Suggested Lifetime of the Key Exchange Session**
   - **Associated Rules: Associated Transmit Rule**
   - **Associated Rules: Associated Receive Rule**

20.3.8.4 VPN - Configured Tunnels - How to Display Rules for all Tunnels

You can have the rules for all configured tunnels displayed in a window.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Tunnels** > **Configured Tunnels**.
4) On the **Display Rules for all Tunnels** tab, you will see detailed information on each configured tunnel such as
   - **Tunnel Data**
   - **Rule Data**
   - **Source Data**
   - **Destination Data**
   - **Service Data**

20.3.8.5 VPN - How to Add a Configured Tunnel

You can add a new IPsec tunnel. A maximum of 256 tunnels can be set up per gateway.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Tunnels** > **Configured Tunnels**.
4) The input window for the new tunnel can be found on the **Add Tunnel** tab.
5) Select **Tunnel Data**.
6) Enter the desired name for the new tunnel under **Name-of-the-Tunnel**.
7) In the **Type of the Local Tunnel Endpoint** drop-down list, select the endpoint address type at the sending end of the tunnel; you can specify a host name or a DNS name.
8) Under **Local Tunnel Endpoint Address**, enter the sender address in a format suitable for the endpoint type.
9) In the **Type of the Remote Tunnel Endpoint** drop-down list, select the type of the endpoint address on the receiving end of the tunnel (only the IP address is currently supported).
10) Under **Remote Tunnel Endpoint Address**, enter the recipient address in a format suitable for the endpoint type. In this field, 0.0.0.0 indicates that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
11) Under **Session Key Handling**, specify the procedure for the key exchange (possible entry: Automatically, using IKE protocol).
12) Select which algorithms (AES or 3DES) may be used under **Suggested Encryption Algorithms**.
13) Select which hash algorithms may be used under **Suggested Hash Algorithms** (MD5, SHA1 or SHA2). The selected algorithms are offered by the initiator of IKE negotiation.
14) Enter the validity period for the session keys to be used under **Suggested Lifetime of the Session Keys**. When this period expires, no more data is exchanged within this session. New session keys are automatically negotiated to replace keys that have become invalid.
15) Enter a validity period under **Suggested Lifetime of the Key Exchange Session**. Once the key exchange session has expired, new keys are automatically negotiated using the IKE protocol.
16) Enter the maximum data volumes for the session keys under **Suggested Data Volume of the Session Keys**. If the data volume is exceeded, new session keys are automatically negotiated using the IKE protocol. If you select **unlimited**, the validity of the session keys will not be limited by the volume of data.
17) Activate the **Key Exchange Data** check box in the upper section of the window.

18) Enter all the key exchange data (**activate 'Perfect Forward Secrecy' and select the VPN Peer Authentication Method (Pre-Shared-Key** or **Digital signatures**)).

INFO: If you have selected **Pre-shared keys** as the authentication method, you will need to enter a 20-character pre-shared key (and repeat this).

INFO: If you want to use **Digital signatures** (from a Lightweight CA) as the authentication method in a VPN network with multiple nodes, you will need to complete some additional configuration steps.

---

a) Create an LWCA certificate at a node.
b) Export the certificate (.crt) to a file.
c) Create and export a certificate revocation list (.crl) to a file.
d) Create and export a peer certificate (.p12) that is signed by a CA for every node.
e) The CA certificate (.crt), the certificate revocation list (.CRL) and the corresponding peer certificates must be imported into every node.

19) Enter the **Suggested Diffie-Hellman Groups** (DH Group 2, 5 or 14).
20) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.9 VPN rules

Rules define how IP packets are to be handled. The rule action *Pass* means that the IP packet is to be transported further (passed through). The rule action *Deny* means that the IP packet will not be transported further (i.e., will be ignored). You can also select whether or not the IP packet will use an encrypted VPN tunnel.

The communication system can manage 640 rules, of which 6 rules are preset (default rules) and 634 are free for allocation.

20.3.9.1 VPN - Active Rules - How to Display Rules

You can have all rules displayed.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Active Rules**.

4) Click on the **Display Rules** tab. You will then see detailed information on the active rules such as

- **Priority**
- **Service**
- **Rule-Based Action**
- **Encryption Required**
- **Rule State**
- **State in IP Stack**
- **Source Address**
- **Destination Address**
- **Tunnels for Encryption**

20.3.9.2 VPN - Active Rules - How to Display Special Rules

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Active Rules**.
4) Click on the desired rule in the menu tree. The **Display Rule** window appears with all the details for this rule (**priority**, **service**, **rule-based action**, **encryption required**, **rule state**, **source address**, **destination address**)

20.3.9.3 VPN - Configured Rules - How to Display all Rules

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Configured Rules**.
4) Click on the **Display Rules** tab. You will then see detailed information on the active rules such as

- **Priority**
- **Service**
- **Rule-Based Action**
- **Encryption Required**
- **Enable Rule**
- **Source Address (type and IP address)**
- **Destination Address (type and IP address)**

20.3.9.4 VPN - Configured Rules - How to Add a Rule

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Configured Rules** > **Add Rule**.
4) Make the settings for the following parameters:
   - **Priority**
   - **Service**
   - **Rule-Based Action (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)**
   - **Encryption Required**
   - **Rule Status**
   - **Source Address - Type**
   - **Source Address - Address (Lowest IP Address in Range)**
   - **Source Address - Subnet Mask (Highest IP Address in Range)**
   - **Destination Address - Type**
   - **Destination Address - Address (Lowest IP Address in Range)**
   - **Destination Address - Subnet Mask (Highest IP Address in Range)**
   - **Tunnel on Receive Side**
   - **Tunnel on Transmit Side**
5) Click on **Apply**.

20.3.9.5 VPN - How to Edit a Rule

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Configured Rules**.
4) Select the rule to be modified in the menu tree.
5) Enter the priority under **Priority**.
6) Enter the service (e.g., DNS) under **Service**.
7) Specify the rule (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**) under **Rule-Based Action**.
8) Enable the **Encryption Required** check box if required.
9) Select the check box **Enable Rule**.
10) Under **Source Address**, enter the **Type** and **IP** address for the edited rule.
11) Under **Destination Address**, enter the **Type** and **IP** address for the edited rule.

12) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.9.6 VPN - How to Add a Rule for the Opposite Direction

When an IPSec rule is created for a transmissions in one direction, the rule for the opposite direction should be added immediately thereafter. The function "Add Rule for the Opposite Direction" copies over the entries of the selected rule, while swapping the source and destination addresses and switching the tunnel assignment accordingly.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Configured Rules**.
4) Select the rule to be edited in the menu tree.
5) Click on the **Add Rule for Opposite Direction** tab.
6) Click on **Apply**.
7) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.9.7 VPN - How to Delete a Rule

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **VPN** > **Rules** > **Configured Rules**.
4) Select the rule to be deleted in the menu tree.
5) Click on the **Delete Rule** tab. The selected rule with all data is displayed.
6) Click on **Delete**. You will receive a warning that you are about to delete this rule.
7) After the entire VPN configuration, the change is applied with **Activate the Configured VPN Tables**.

20.3.10 PKI Server

The PKI server designates a server that can issue, distribute and verify digital certificates. The certificates issued within a PKI (Public Key Infrastructure) are used to protect communications.

When using certificates (digital signatures), an attempt is made to download the CRL via the PKI URL configured by the PKI server.

20.3.10.1 VPN - How to Display the PKI Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Public Key Infrastructure (PKI)**.
4) Click on the **Display PKI Servers** tab. The **Name of the PKI Server**, the **PKI Server Type** and the **URL of the PKI Server** are displayed.

20.3.10.2 VPN - How to Add a PKI Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **VPN** > **Public Key Infrastructure (PKI)**.
4) Click on the **Add PKI Server** tab.
5) Enter the **Name of the PKI Server**.
6) Enter the **PKI Server Type** (e.g., LDAP).
7) Enter the **URL of the PKI Server**.
8) Confirm your entries and click **Apply**.

20.4 Certificate Handling

Certificate handling (for Secure Sockets Layer, SSL) promotes the reliable administration of the communication system. The data cannot be read or manipulated by unauthorized parties. Certificates are used for authorization. You can generate and administer certificates.

Administrative access is encrypted over HTTPS using the TLS 1.2 protocol. Certificates are used to authenticate the communication system. By default, a self-signed certificate is used. A customer-specific certificate can be used to enhance security.

SSL supports the following security services:

- Authenticity (the communication partner is who he says he is)
- Trustworthiness (the data cannot be read by a third party)
- Integrity (the data was received in the same condition as it was sent)

These security services demand prior agreement on the security mechanism used and the exchange of cryptographic keys. These two tasks are performed in the course of connection setup.

SSL uses certificates and keys to guarantee secure data transmission.

CRL (Certificate Revocation List)

Certificate Revocation Lists (CRL) are files containing a list of blocked certificates, their serial number, and their blocking data. A CRL list also contains the name of the party who issued the certificate revocation list and the next authentication time.

CDP (CRL Distribution Point)

The CRL Distribution Point (CDP) is the directory (location) where the current versions of the CRLs are located (for example, http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

System-Specific Information

Client/server communication in SSL-based administration.

The server uses the certificates generated or imported by the WBM for authentication at the client. Such certificates can be imported into the browser as trusted certificates to avoid warning messages in the browser when connecting to the SSL server.

INFO: The SSL certificate generation can also be used for SPE.

20.4.1 Introduction

What are SSL certificates?

TLS/SSL certificates are used to protect data during communication between servers such as OpenScape Business and web-based clients by means of encryption and to verify the identity of the company belonging to the website so that the user can be sure that he is really communicating with the real server.

OpenScape Business issues itself a temporary ("self-signed") SSL certificate during the initial system installation or upon change of the LAN IP address, but this certificate does not contain sufficient data for identity verification apart from the user's own LAN IP address.

Such a certificate does not comply with current security standards and must be replaced by a trustworthy, individual SSL certificate issued by an official Certificate Authority (CA) as soon as possible after the initial installation of OpenScape Business. This is the only way to meet the minimum standards of current client operating systems and web browsers for secure Internet communication.

CA’s usually offer SSL certificates with different trust levels: Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). For OpenScape Business, domain validated certificates are sufficient. This is usually the cheapest option, with some CA’s even free of charge.

For which web services does OpenScape Business use the SSL certificate?

The active SSL certificate is used for administrator access via the Admin Portal as well as for various other web-based applications (e.g. key programming) and WSI-based UC clients such as myPortal @work, myPortal to go, Application Launcher, myContacts and myPortal for Teams.

Where can I get a trusted SSL certificate from?

To obtain an SSL certificate, you must contact a certification authority. You must verify the domain name used to reach OpenScape Business in order to create a Certificate Signing Request (CSR), which is then sent to the CA for validation.

It should be noted that CA issued, trusted SSL certificates only have a limited validity period of a few months to a few years to ensure that they comply with current security standards. It is important to keep an eye on the expiration date and to renew SSL certificates before the expiration date is reached.

Failure to renew SSL certificates can result in the client environment classifying the website as "insecure" and preventing communication with the server.

Please note that some client environments have special requirements for SSL certificates, which may not be met by every CA. Such special requirements are linked further down in the section „client side considerations“. When selecting your CA, please follow the corresponding instructions.

Why has the certificate issue become so important?

The use of trustworthy, customer or server-specific SSL certificates is extremely important and is increasingly being enforced by the major operating system and browser manufacturers. Security, professionalism, integrity and confidentiality when handling personal data are the key arguments for this.

Due to the increasing use of web-based services and clients, including via the Internet, the permanent use of the temporary, self-signed (and therefore insecure) default SSL certificate of OpenScape Business is out of the question.

In addition, the temporary, self-signed certificate of OSBiz has a multi-year validity, while some client environments have started restricting the certificate validity – sometimes to not more than one year.

Moreover, in many customer installations that were originally set up with older software releases prior to V3R2.1, the validity of these temporary, self-signed certificates expires on January 1, 2024.

The Admin Portal of OpenScape Business provides a range of tools for generating and managing SSL certificates and also supports the system administrator in creating certificate signing requests. The most important functions in this regard are explained below.

20.4.2 How to Generate CA Certificates

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **Security**.

3) Navigate in the menu tree down to **SSL** > **Certificate Generation**.
4) Click on the **Generate CA Certificate** tab.
5) Specify the **Name of the Certificate**.
6) Enter a serial number also in the field **Serial Number of Certificate**.
7) Select the algorithm under **Type of Signature Algorithm** (**sha256RSA**, **sha512RSA**).
8) Select the public key under **Public Key Length**.
9) Enter the start and end of the validity period in the relevant fields.
10) Then complete the fields **Subject Name** or **Subject Alternative Name**.
11) Enter the **CRL Distribution Point**.
12) Click on **Apply** followed by **OK**.

20.4.3 How to Generate Self-Signed Certificates

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Generation**.
4) Click on the **Generate Self-Signed Certificate** tab in the **Certificate Generation** window.
5) In the field **Certificate Name**, assign a name for the generated certificate.
6) Enter a serial number also in the field **Serial Number of Certificate**.
7) Select the algorithm under **Type of Signature Algorithm**.
8) Select the public key under **Public Key Length**.
9) Enter the start and end of the validity period in the relevant fields.
10) Then complete the fields **Subject Name** or **Subject Alternative Name**.
11) Enter the **CRL Distribution Point**.
12) Click on **Apply** followed by **OK**.

20.4.4 How to Generate Certificate Signing Requests (CSR)

Dependent on the certificate authority of your choice, there are different options to create certificate signing requests online (e.g. via a CA's web portal) or offline. The OpenScape Business Admin Portal offers an option to create a CSR for download and transmission to the CA.

Prerequisites

You are logged into the WBM with the **Expert** profile.

In Generate Certificate Signing Request (CSR) page, the following fields must be filled in order to generate the key and csr files.

General:

Certificate Request Name: A name for the CSR which will be used in the name of the file that will be downloaded.

Type of Signature Algorithm: Select between sha256RSA and sha512RSA

Public Key Length: The only option is 2048

Country (C): Use a two letter country code e.g. DE

Organization (O): denotes the formal name of the overarching entity or company to which the certificate is assigned.

Organization Unit (OU): designates a specific subunit or department within an organization, offering additional granularity to identify the organizational structure.

Common Name (CN): a vital identifier, usually representing the domain name for which the certificate is issued, providing a key element for verifying the certificate holder identity.

Subject Alternative Name (Optional):

The Subject Alternative Name (SAN) extension is a feature of X.509 certificates used in the field of cryptography. X.509 is a standard that defines the format of public-key certificates. The SAN extension allows additional identities, such as host names, IP addresses, or email addresses, to be associated with a single X.509 certificate. This is particularly useful in scenarios where a server may be accessed by different names or addresses.

Distinguished Name Format: Information similar to the Subject name such as Country (C), Organization (O), Organization Unit (OU), Common Name (CN) must be filled.

Other Format:

Subject Alternative Name Extension: Option are DNS Name, IP Address, Email Address, Uniform Resource Indicator, Other

Subject Alternative Name: The SAN extension helps address limitations in cases where a single common name is insufficient or when there is a need to include multiple identities within a single certificate. This is important for modern web services, where a server might be accessible through multiple domain names or IP addresses.

Here's an example of how the SAN extension might look in a certificate:

Subject Alternative Name:

DNS:www.example.com

DNS:mail.example.com

IP Address:192.168.1.1

Email:admin@example.com

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) In the **Generate Certificate Signing Request (CSR)** tab:

5) Enter the name of the certificate on the **Certificate Request Name** field.
6) Click to select either **sha256RSA** or **sha512RSA** from the **Type of Signature Algorithm** drop-down list.
7) **Public Key Length** is fixed to **2048** characters.
8) Enter the country **Country C**.
9) Enter the organization **Organization O**.
10) Enter the **Organization Unit (OU)**.
11) Enter the **Common Name (CN)**.
12) Click on either **Distinguished Name Format** or **Other Format**, to select the certificate format.
13) Optionally, choose on of the values for **Subject Alternative Name Extension**.
14) Optionally, click on the **Add** button to add a **Subject Alternative Name** in the CSR.
15) Click on **Apply** followed by **OK**.

20.4.5 How to Import Server Certificates (PKCS#12)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the **Import Server Certificate (PKCS#12)** tab in the **Server Certificates** window.

NOTICE: If other format is selected, more than one SAN entries is possible to be configured.

---

5) Enter the **Name of the Certificate**.
6) Enter the **Passphrase for decryption**.
7) Under **File with Certificate**, enter the desired certificate file by using the **Choose File** button.
8) Click on **Import Certificate from File** followed by **OK**.

20.4.6 How to Import Server Certificates (PEM)

Certificates in PEM format are supported as an alternative. You can do so by importing the certificate and the key file as two separate files.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the **Import Server Certificate (PKCS#12)** tab in the **Server Certificates** window.

NOTICE: If other format is selected, more than one SAN entries is possible to be configured.

---

5) Under the **Import Certificate and Key files** section:
6) Enter the **Name of the Certificate**. (You can enter a name of your own choice.)
7) Enter the **Passphrase for decryption**. (You can enter a passphrase of your own choice.)
8) Under **Certificate File**, choose the certificate file by using the **Choose File** button.
9) Under **Key File**, choose the key file by using the **Choose File** button.
10) Click on **Import Certificate and Key** followed by **OK**.

20.4.7 How to Display Certificates

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the required certificate. The **Server Certificates** window appears.
5) Click on the **View Certificate** tab to view the current certificate.

20.4.8 How to Delete Certificates

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the required certificate The **Server Certificates** window appears.

5) Click on the **Delete Certificate** tab. The name of the certificate currently valid appears with a warning that you are about to delete it.
6) Click on **Delete** if you are sure you want to delete the certificate.

20.4.9 How to Export Certificates (X.509)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the required certificate. The **Server Certificates** window appears.
5) Click on the **Export Certificate (X.509)** tab. You can open or save the certificate.

20.4.10 How to Import Updated Certificates (X.509)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the required certificate. The **Server Certificates** window appears.
5) Click on the **Import Updated Certificate [X.509]** tab. The name of the certificate currently valid appears.
6) Enter the required certificate in the **File with Certificate** field or select **Browse**.
7) Complete your input with **Fingerprint of**.

20.4.11 How to Activate Certificates

With this function, you specify the certificate to be use for web-based administration.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Click on the required certificate.
5) Click on the **Activate Certificate** tab. A warning appears that this action will interrupt all ongoing HTTP connections.
6) Select the desired system (OpenScape Business, UC Booster Server, UC Booster Card) for which you want to enable the certificate in the **System** drop-down list.

NOTICE: To work properly, the IP address of the system must be entered in the **Common Name** field in every certificate. Make sure that you enable the correct certificate for the selected system.

---

7) Click on **Activate Now**.

NOTICE: The imported Server Certificate must be issued directly from a Root CA. Intermediate CAs must not be used.

20.4.12 Certificate Handling for Booster Server

When initially installing a Booster Server, a certificate is created with the IP address of the booster serving as the common name. The certificate has a 10-year validity period and is issued for the organization "Unify Software and Solutions GmbH & Co. KG," with the organizational unit specified as "Unify."

It is possible to replace the default certificate on the Booster Server by transferring a different certificate through the Web-Based Management (WBM) interface of the system. Once transferred, the new certificate can be activated, providing an alternative security configuration for the Booster Server.

NOTICE: Similarly, if your system uses UC Booster Card (OCAB) instead, you can choose **UC Booster Card** from the drop-down menu of **step 6**.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Security**.
3) Navigate in the menu tree down to **SSL** > **Certificate Management** > **Server Certificates**.
4) Choose one of the imported certificates.
5) Navigate to the **Activate Certificate** tab.
6) From the system drop-down menu, select **OpenScape Business UC Booster Server**.
7) Click the **Activate Now** button to apply the selected certificate to the Booster Server.

20.5 Web Security

The web access filter can be found under Web Security. It allows you to manage client permissions as well as the admin log which keeps track of any access or change to the communication system.

20.5.1 Connections to the Web Server

The connections of the clients (e.g., myPortal to go) to the internal web server of the communication system can be either encrypted (HTTPS) or unencrypted (HTTP).

NOTICE: Unencrypted connections to the web server may allow unauthorized access to sensitive data! For security reasons, it is strongly recommended that only an encrypted connection (HTTPS) be used when working with myPortal to go (Web Edition) over the Internet.

Only an encrypted connection to the web server is available for myPortal to go (App Edition).

20.5.1.1 How to Configure Connections to the Web Server (UC Suite)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Security**.
3) Navigate in the menu tree to **Web Access**.
4) Configure the connections to the web server:
   - If you want to enable encrypted connections, select the check box **HTTPS**.
   - If you want to enable unencrypted connections, select the check box **HTTP**.
5) If appropriate, enable **Save login data to device** if you want to allow this function. This causes the login credentials in the web browser of the mobile phone to be saved using cookies.
6) Click on **Save**.

20.5.1.2 How to Configure Connections to the Web Server (UC Smart)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click on **Applications** > **UC Smart** > **Basic Settings**.
3) Make sure that UC Smart is **Active**.
4) Configure the connections to the web server:
   - If you want to enable encrypted connections, select the check box **HTTPS**.
   - If you want to enable unencrypted connections, select the check box **HTTP**.
5) Click on **Apply**, followed by **OK**.

20.5.2 Admin Log (also called Admin Protocol)

The Admin log enables you to track what changes were made to the communication system and by whom and when.

20.5.2.1 How to Load the Admin Log

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** in the navigation tree.
3) Navigate in the menu tree to **Admin Log** > **Admin Log Data**.
4) The message "The admin log will be transferred from the system" appears in the **Admin Log Data** window. Please confirm".
5) Click on **Load**.

20.5.2.2 How to Change the Admin Log Language

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Service**.
3) Navigate in the menu tree to **Admin Log** > **Configuration**.
4) Set the desired language in the **Edit Configuration** window under **Admin Log Language**.
5) Click on **Apply**.

20.6 SQL Security

OpenScape Business stores system configuration data, call data records, user account credentials, UC data etc. in an internal SQL database. Access to the database is protected by login credentials.

Up to SW version V2R2 the used login credentials are protected by a password, which could not be changed by an OpenScape Business administrator. From V2R2 on the password can be changed.The password is machine generated and is not shown to the administrator. For compatibility within multinode scenarios running old SW versions, it possible to change back a modified password to the “old” value.The SQL access password configuration can be found under SQL Security. The SQL access password configuration can be used both in network and single node environments. The handling for specific single node or multinode scenarios is described with the subsequent chapters.

20.6.1 Single node

SW Upgrade from V2R1 or older

After a SW upgrade from V2R1 the OLD SQL database password is active.The SQL password has to be changed within the new software version by the system administrator using the Administration Portal (WBM).

Setup of new system

When the date is set up in the system for the first time, a new SQL password will be generated. Only the first time the date and time is set, is when the SQL password is changed automatically.

Setup of a reloaded "single node" system

After each system reload the OLD SQL database password is active within the system.The SQL password has to be changed within the new software version by the system administrator using the Administration Portal (WBM).

20.6.2 Multinode

The single node system is configured and integrated in the network in the known manner. After system setup the new slave node synchronizes its SQL password with the master node. No action is required to adapt the SQL password within the slave node.

Reload of a V2R2 or higher node within V2R2 or higher Network

After a reload of a network node within the network, the node has to re-configured and integrated again into the network.

Reload of the Master Node

In case of a master node the SQL password has to be changed by the system administrator using the Administration Portal (WBM). All slave nodes synchronize their SQL password with the new one within the master node. No action is required to change the SQL password within the slave nodes.

Reload of the Slave Node

In case of a slave node no action is required as the slave node synchronizes its SQL password with the master node.

New V2R2 or higher slave node within V2R1 Network (not recommended scenario)

The single node system is configured and integrated in the network in the known manner. After system setup the new slave node detects that the master node uses the old SQL password and uses the old SQL password as well. No further action is required to adapt the SQL password within the slave node.

NOTICE: It is strictly recommended to upgrade the whole network to the latest software version.

New V2R2 or higher master node within V2R1 Network (not recommended scenario)

The master node system is configured and integrated in the network in the known manner. After system setup the new master node uses the old SQL password. The system administrator may not change the old password, as the V2R1 slaves are not able to synchronize with a new SQL password in the master node. In this case the node would not work together within the network.In case that system administrator has change the SQL password by hazard he has to switch back to the “default” password within the master node configuration.

NOTICE: It is strictly recommended to upgrade the whole network to the latest software version.

20.6.3 How to Configure Passwords to the SQL Database

Prerequisites

You are logged into the WBM with the **Expert**.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony Server** > **Security**.
3) Navigate in the menu tree to **SQL Security**.
4) Configure the passwords to the SQL database:
   - If you want to generate a new password not known to the user, select the box **Generate new**.
   - If you want the default password to be activated, select the box **Activate default**.

NOTICE: In the landing page notification area, the following message will be displayed if the default sql password is used

(or a password generated with the old password generation algorithm):

'`Default SQL password is in use. Please consider changing it via Expert mode`'

The message is a URL link that leads to the SQL Security page in orden to change it.

20.7 SIP Attack Protection

The so-called SIP attacks represent a new form of attacks on communications systems via IP telephony. Such attacks may occur either from the LAN or via the Internet (through badly configured routers). Protection against SIP attacks is provided through password-protected SIP access.

The following rules should be applicable for any SIP subscriber access:

- Active authentication
- A qualified password that
- – is between 8 and 20 characters in length
  – includes one or more uppercase letters (A to Z)
  – includes one or more lowercase letters (A to Z)
  – includes one or more digits (0 to 9),
  – includes one or more special characters (e.g.: %),
  – does not have more than 3 repeated characters
- Definition of a SIP station ID that differs from the station number.

When a new SIP station is set up, authentication is activated by default, and a random password is generated. Since this random password is not known, it must be changed by the administrator.

The relevant settings in the communication system are made using the "Central Telephony" wizard or Manager E.

During system startup, the password list is checked, and an entry is made in the EventLog (Event Viewer) if a SIP station is configured without a password.

INFO: If the communication system is used as an Internet router, port 5060 must be closed (default setting). For Internet telephony via an ITSP, the communication system opens the relevant ports and keeps them open.

Port 5060 must likewise be closed If an external router or firewall is being used. The communication system is responsible for opening this port (if required).

21 Networking OpenScape Business

OpenScape Business communication systems can be networked with one another and additionally with the communication systems OpenScape 4000 (HiPath 4000) and OpenScape Voice as well. In a homogeneous OpenScape Business network, subscribers can now use features such as the presence status, voicemail, conferencing and much more in exactly the same way as was originally possible with only a single OpenScape Business communication system.

Possible Networks:

- Pure voice network of OpenScape Business X
- OpenScape Business X and S OpenScape Business networking (optionally with UC Suite or UC Smart).
- OpenScape Business X with OpenScape 4000 (UC functionality in OpenScape Business only under certain conditions)
- OpenScape Business X with OpenScape Voice (without UC functionality in OpenScape Business)
- Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection.
- Networking via ISDN
- OpenScape Business inter-network with central ITSP trunk connection

The communication systems are prepared for networking with the **Networking Configuration** wizard. In this wizard, it must be specified whether a master or slave node is involved. In addition, 16 lines are automatically assigned to route 16 (networking).

All networks that use unified communications features (such as UC Smart or UC Suite, for example) must be based on a closed numbering plan. Networks without unified communications features can be based on an open or closed numbering plan. In order to respond flexibly to future extension requests from customers, it is recommended to always use closed numbering for any newly created internetwork.

INFO: Configuring an IP network is a complex task and should only be performed by experienced service technicians.

It is not possible to set up a pure OpenScape Business X1 internetwork, since an X1 system cannot be a master system, and there always needs to be a master system in the internetwork.

A network of OpenScape Business with the following systems is not supported:

- HiPath 3000 SIP-Q; only TDM networking based on S_0/S_{2M} with CorNet NQ is supported; see Networking via ISDN,
- HiPath 5000 RSM
- OpenScape Office MX
- OpenScape Office LX

The migration from a HiPath 3000 (including HiPath 5000 RSM) to OpenScape Business is described in the section on Migration.

NOTICE: For information regarding licensing and upgrating or migrating systems in a network, please see **Network - Licensing** section in Updates chapter.

21.1 Network Plan

Before configuring an internetwork, a network plan should first be created after consulting with the customer.

The network plan should include the following data:

- Node ID (node number) and the associated IP addresses
- Dial plan

21.1.1 Homogeneous and Heterogeneous Networks

In general, a distinction is made in networking between homogeneous (where all components belong to a single system family) and heterogeneous networks (with different systems).

Homogeneous (Native) Network

Heterogeneous (Hybrid) Network

A homogeneous (native) network consists of components of the OpenScape Business systems family.

A heterogeneous (hybrid) network consists of components of the OpenScape Business systems family and an OpenScape 4000 or an OpenScape Voice, for example.

Overview of all OpenScape Business Nodes in the Network

All OpenScape Business nodes in an internetwork can be displayed via the **Networking** entry in the navigation bar of the WBM. In addition, all the OpenScape Business stations of the internetwork can be displayed sorted by node.

The following information can be displayed:

- **Node ID**: Node ID
- **M** / **S**: Identification to indicate whether the node is a Master or Slave
- **Net name**: name of the node
- **Type**: type of the node (**OSBiz X**: hardware model, **OSBiz S**: softswitch)
- **OSBiz X / OSBiz S**: IP address of the node, clickable (opens the WBM of the node)
- **Application Server**: IP address of the UC server (UC Booster Card or UC Booster Server)
- **Registration status**: status of the registration
- **Alive**: Displays whether the node is active or not

21.1.1.1 How to Display the Overview of all OpenScape Business Nodes

Prerequisites

Multiple OpenScape Business communication systems are networked with one another.

Step by Step

1) In the navigation bar, click on **Networking**.
2) Click on **Domain View** in the navigation tree. All OpenScape Business nodes in the internetwork are listed.

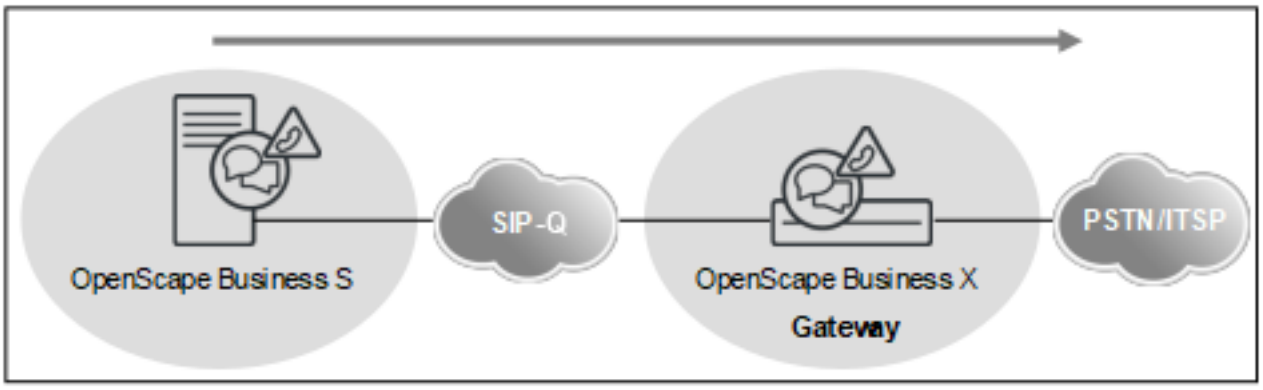
21.1.2 Single and Multi-Gateway

In homogeneous OpenScape Business networks, a distinction is made between a single network and multi-gateway network, depending on whether only a single gateway or multiple gateways are used.

Single Gateway

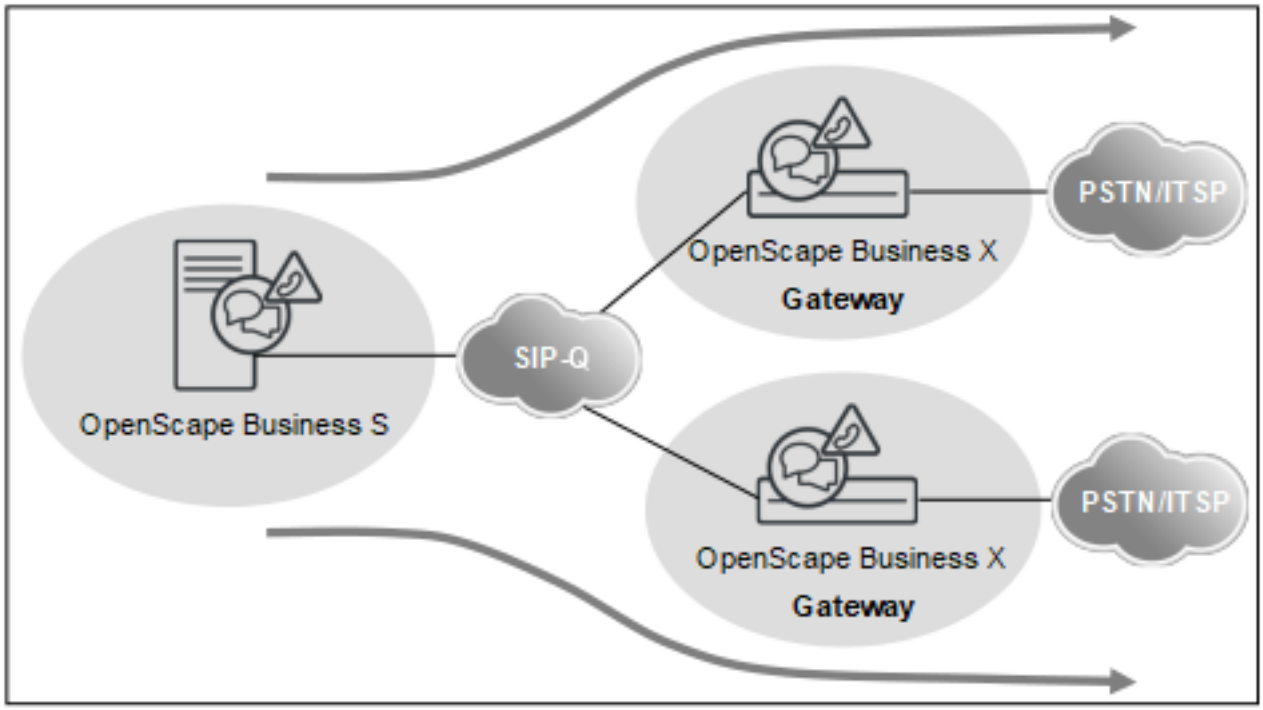
Multi-Gateway

In the case of a single-gateway network, calls from and to the server are routed via a single gateway. All IP stations that are registered at the server use this single gateway.



- Supported if there are one or more OpenScape Business S systems in the network.
- The IP stations are connected to different communication systems.
- OpenScape Business X is used as a gateway.

In the case of a multi-gateway network, calls are routed via several different OpenScape Business gateways.



- There is only one PSTN Provider and one CO station number per gateway.
- The stations of the different locations are registered at a central system (OpenScape Business S).
- Every station of the OpenScape Business S is assigned a specific gateway (OpenScape Business X).
- There must only be a single OpenScape Business S in the network.
- OpenScape Business and OpenScape Business S are in the same time zone and in the same country (same country code).
- There is only one CO access code netwide.
- ISDN and analog stations, for example, can be locally set up on the gateways.

21.2 Network-wide Features

Network-wide voice features are essentially determined by the SIP-Q networking protocol. Network-wide UC features are determined by the networking of the UC solution (UC Suite or UC Smart) and their UC clients.

21.2.1 Network-wide Features of the UC Solutions

The following table provides you with an overview of the network-wide features of both the UC solutions, UC Smart and UC Suite.

UC interworking using both OpenScape 4000 and OpenScape Voice is not possible. In an OpenScape Business internetwork, either UC Smart or UC Suite should be used. Mixed UC solutions are not supported.

Network-wide UC features	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Network-wide visibility of the Presence status (presence management)	x	x	x	x	x
Change of own presence status via the client	x	x	x	x	x
Change of own presence status via the TUI	x	x	x	x	x
Status-based call forwarding	x	x	x	Via destinations defined in other UC Suite Clients	Via destinations defined in myPortal
Network-wide status display in Favorites	x	x	x	x	x
Network-wide status display in directories	x	x	x	x	x
Network-wide status display in the Journal	-	-	x	-	-
Enable CallMe service	-	-	x	x	x
Calendar integration (Outlook)	-	-	x	-	-
Calendar integration (iCal) (only with myPortal for Desktop)	-	-	x	-	-
Network-wide display of the call status (free, busy, ringing state)	x	x	x	x	x
Creation of network-wide groups	x	x	x	-	-
Compact display of favorites	-	-	x	-	-
Conversations	x	-	-	x	-
Personal directory	Local	Local	Local	Local	Local
Internal directory	Local	Local	Local	Local	Local
External directory	-	-	x	x	x
Searching in directories on a network-wide basis	x	x	x	x	x
Access to speed-dial destinations defined in the system (SSD)	Local	Local	-	Local	Local

Network-wide UC features	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Import/Manage personal contacts (CSV/XML)	x	-	x	-	-
Access to Outlook Contacts	x	-	x	-	-
Import personal contacts (Mac OS) (myPortal for Desktop)	-	-	x	-	-
Integration of external directory server via LDAP	-	-	x	-	-
All calls	x	x	x	x	x
Open calls	-	x	x	-	-
Missed calls	x	x	x	x	x
Answered calls	x	x	x	x	x
Scheduled calls	-	-	x	-	-
VoIP calls	x	-	x	x	-
Fax journal	-	-	x	-	-
Manual dialing	x	x	x	x	x
Desktop dialer (click to call)	-	-	x	-	-
Forwarding	x	x	x	x	x
Place call on hold	x	x	x	x	x
Record calls (voice recording)	-	-	x	-	-
Send e-mail	x	x	x	x	x
Send SMS	-	x	-	-	x
Popups	x	-	x	x	-
AdHoc conference	x	x	x	x	x
Scheduled conferences	-	-	x	-	-
Permanent and open conferences (drag & drop conference)	x	-	x	-	-
Web Collaboration Integration	x	-	x	x	-
Voicemail box (visual voicemail)	x	x	x	x	x

Network-wide UC features	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Listen to voicemail via telephone	x	x	x	x	x
Listen to voicemail via PC sound card	-	-	x	-	-
How to Send a Voice Message as an E-mail	x	x	x	-	-
Fax (for Windows operating systems)	-	-	x	-	-
Instant messaging (chat) network-wide	x	-	x	-	-

21.2.2 Network-wide Voice Features

For networking via the SIP-Q protocol, the following voice features are supported for OpenScape Business and other communication systems.

Feature	SIP-Q (IP Network)
Basic call	Yes
Callback on busy	Yes
Callback on RNA	Yes
Override	Yes
Call waiting	Yes
Second call	Yes
Calling Line Identification Presentation (CLIP)	Yes
Calling Line Identification Restriction (CLIR)	Yes
Connected Line ID Presentation (COLP)	Yes
Connected Line ID Restriction (COLR)	Yes
Calling / Connected Name Identification Presentation (CNIP)	Yes
Calling / Connected Name Identification Restriction (CNIR)	Yes
Do Not Disturb	Yes
Call forwarding	Yes
Call Forwarding on Busy	Yes
Call Forwarding on RNA	Yes
Call Deflection	Yes
Advice of Charge at Call Setup	no

Feature	SIP-Q (IP Network)
Advice of Charge during Call	Yes
Advice of Charge at the end of the call	Yes
Path optimization	no
Rerouting	no
Message Waiting Indication / Info	Yes
Trace call	Yes
Hold	Yes
Toggle/Connect	Yes
Transfer	Yes
Conferencing	Yes
Automatic Recall	Yes
Calling for Help	Yes
Intercept	Yes
Private Numbering Plan (PNP)	no
Call pickup	no
Hunt Group	Yes
SPE (except for conferencing and applications)	Yes

21.3 Licensing an Internetwork

For a networked communication system, central licensing can be selected.

All licenses of the individual systems are combined into a network-wide license at the license server. In the internetwork, the licenses can be assigned freely to the individual nodes using the WBM.

For more information, see Licensing Multiple Communication Systems (Internetwork) .

21.4 Networking Requirements

To ensure the quality of the voice transmission, the IP networks being used and the communication system must meet certain requirements. The voice quality and voice communication reliability always depend on the network technology in use.

Network Parameters, LAN and WAN Requirements

Parameters	Minimum requirement	Notes
Delay (one way)	50 ms	Higher values degrade the voice quality.
Round Trip Delay	100 ms	Higher values degrade the voice quality.
Jitter	20 ms	Higher values degrade the voice quality.
Packet Loss	3%	For fax or modem transmissions using G.711, the packet loss should not exceed 0.05% (in the event that no T.38 is possible).
Consecutive Packet Loss	3 with G.711	Higher values degrade the voice quality.

Recommendation for Calculating Bandwidth

- A bandwidth of at least 256 kbps (in both the sending and receiving direction) is required on the internetwork.
- The bandwidth calculation should be based on a maximum of 50% for the voice portion with respect to the total bandwidth. In other words, in the case of a 1 Mbit WAN, for example, a maximum of 500 kbps should be calculated for voice. With the G.711 codec, for example, that would be a maximum of 5 IP trunks.
- Regardless thereof, the network properties with respect to QoS, delay, packet loss, etc., must also be taken into account.

21.4.1 LAN Networking Requirements

To ensure the quality of the voice and data transmissions, the IP networks being used and the communication system must meet certain requirements for the LAN.

LAN requirements

The data network must be of the Ethernet type:

- The recommended cable is at least a Cat.5 cable (screened/unscreened multi-element cables characterized for up to 100 MHz for horizontal and building backbone cables as per EN 50288).
- Support for QoS: IEEE. 802.1p, DiffServ (RFC 2474).
- All active LAN ports must support 100 / 1000 MBit/sec. and full duplex communications.

Every communication system must be connected via a switch or a dedicated port of a router. Hubs and repeaters are not supported.

Payload Connections with RTP (Real-time Transport Protocol) in a LAN Environment

The required bandwidth for voice transmissions in an IP network can be calculated with the help of the following table:

Codec type	Packet parameters	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl. header) (kbps)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82.7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73.3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17.3
RTCP		5000		280		0.4

The load in the LAN applies to both the sending and receiving direction.

The calculation includes VLAN tagging in accordance IEEE 802 1q. Without VLAN tagging, the packet length is shorter by 4 bytes.

The overhead is calculated as follows:

Protocol	Bytes
RTP Header	12
UDP Header	8
IP Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Total	70

Payload transport in a T.38 LAN environment:

	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	Payload packet (overhead in percent)	Ethernet load (incl. header) (kbps)
T.38	30	169	227	34%	60.5

Payload Connections with SRTP (Real-time Transport Protocol) in a LAN Environment:

Codec type	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	SRTP Ethernet packet length (kbps)	RTP Ethernet packet length (kbps)	Additional bandwidth for 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

Codec type	Sample Rate (ms)	Payload (bytes)	Ethernet packet length (bytes)	SRTP Ethernet packet length (kbps)	RTP Ethernet packet length (kbps)	Additional bandwidth for SRTP (%)
G.729A	40	40	124	24.8	22	12.7
G.729A	60	60	144	19.2	17.3	10.8

21.4.2 Dial Plan in the Network

The dial plan is an important prerequisite for networking. The complexity of the internetwork configuration depends on the dial plan. OpenScape Business generally supports open and closed numbering in an internetwork. It should be noted, however, that the full scope of UC features can only be used only with closed numbering.

Closed numbering

In the case of closed numbering, a station in the internetwork is uniquely identified by the station number. Each station in the internetwork can reach another station by directly dialing its station number.

The advantage of closed numbering is that you do not have to dial a node number to reach another station in another networked communication system.

Table 10: Examples of closed numbering

	Node 1	Node 2	Node 3	Node 4
Phone Numbers	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Open numbering

In open numbering, a station is uniquely identified by the node number and the station number. Users of different communication systems (nodes) in the internetwork can thus have the same station number.

With open numbering, the station's node number must always be dialed in addition to the phone number. Phone number ranges can be used more than once for this, and multiple phone numbers can be used.

The following UC features are not supported with open numbering:

- UC Smart
- UC Suite
- network-wide CSP (CSTA Service Provider)
- DSS server
- CMD (CSTA Message Dispatcher)

Table 11: Examples of Open Numbering

	Node 1	Node 2	Node 3	Node 4
Node number (PABX number)	95	96	97	98
Phone Numbers	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

21.4.2.1 Dialing Public Phone Numbers in the Network

Regardless of whether a closed or open numbering system is being used, it makes sense to dial both node and network-internal destinations using public phone numbers (e.g., as a UC client that dials contacts in the fully-qualified format from directories).

21.5 Path Optimization (Path Replacement)

Path optimization (also called path replacement) helps to avoid the dual seizure of IP trunks for networked communication systems.

When multiple OpenScape Business systems are networked, the following problem could occur, for example: First, let us assume that subscriber A calls subscriber B who, in turn, has forwarded all calls to subscriber C. Subscribers A and C are in the same network node, but subscriber B is on a different network node. Consequently, the call with call forwarding initially seizes two trunks between the two network nodes. To avoid this dual seizure, path optimization must be enabled.

INFO: The system flag for the path optimization must be enabled for all networked OpenScape Business systems.

INFO: It is strongly advised to not use Path Replacement feature in networks where analogue fax stations are used. This limitation will be raised with an upcoming software version.

The path optimization is performed:

- Within the OpenScape Business network segment
- After the connection setup (not in the ringing phase!)
- After transfer scenarios
- After call forwarding and CFNA (call forwarding-no answer)

The path optimization is not performed:

- When a ringing group or group call is involved
- For conferences
- If some other feature is enabled when executing the path optimization, the optimization is aborted.
- For inhomogeneous networking, the external systems are configured via the SIP interconnection. In this case, regardless of the configuration of the flag, no path replacement is possible (e.g., OpenScape 4000, OpenScape Voice, external SIP servers).

21.5.1 How to Enable or Disable Path Optimization (Path Replacement)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click on **System** > **System Flags**.
4) Select one of the following options:
   - If you want to allow a call pickup for recalls, enable the **Path optimization** check box.
   - If you do not want to allow a call pickup for recalls, clear the **Path optimization** check box.
5) Click on **Apply** followed by **OK**.

21.6 Networking Scenarios

There are several scenarios how OpenScape Business systems can be networked with one another and with other communication systems.

- Networking Multiple OpenScape Business X Systems
- Networking OpenScape Business X and OpenScape Business S (Single Gateway)
- Networking OpenScape Business X and OpenScape Business S (Multi-Gateway)
- Networking of OpenScape Business S in a Hosting Environment
- Networking OpenScape Business X and OpenScape Voice
- Networking OpenScape Business X and OpenScape Voice
- Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection
- Open Numbering in OpenScape Business X Networks
- Networking via ISDN
- OpenScape Business internetwork with central ITSP trunk connection

Call charge details can only be retrieved per network node, but not across nodes.

21.6.1 Dependencies and Restrictions

It is important to note some dependencies and constraints on the possible networking scenarios.

Dependencies and Restrictions

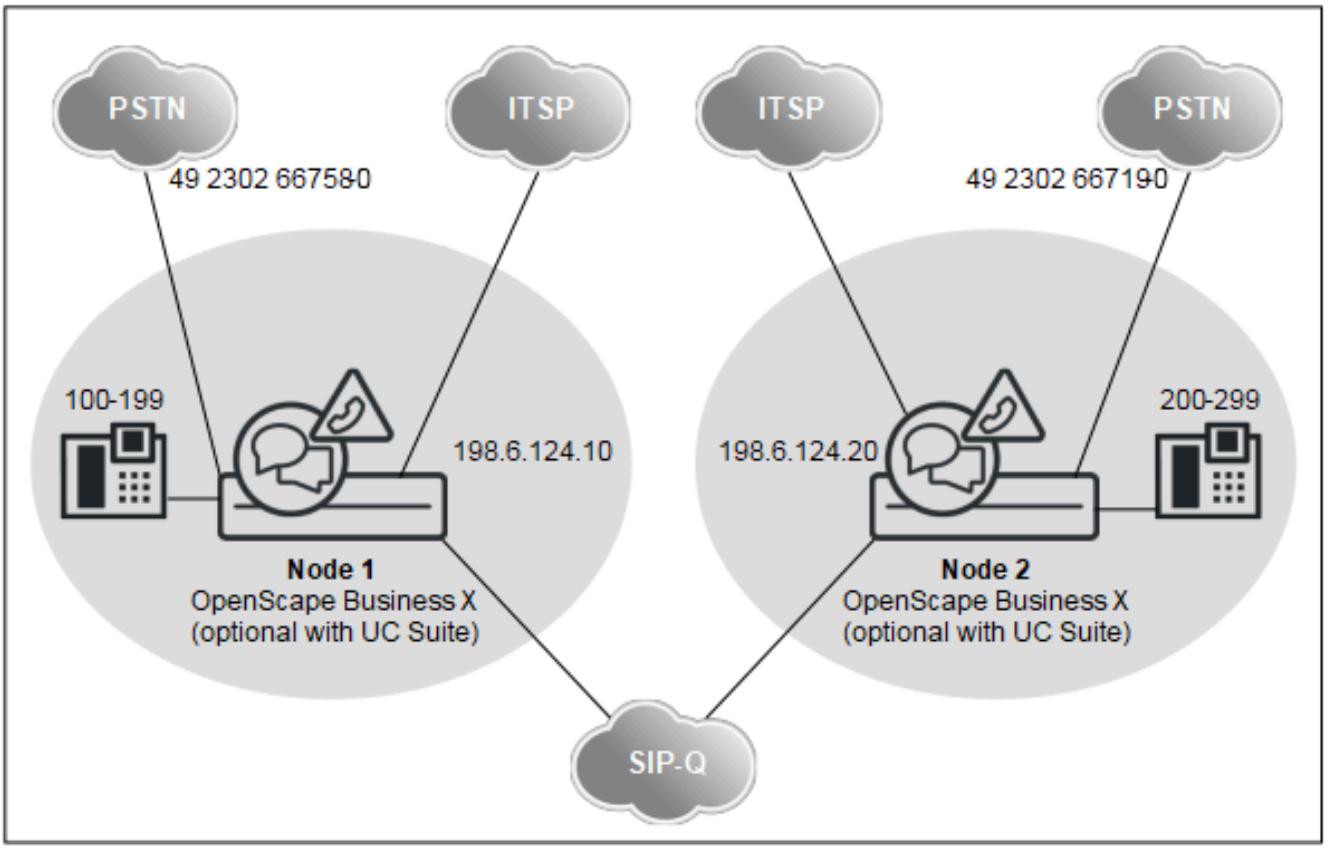
- Every system in the internetwork is assigned its own time zone. Consequently, all stations in a system have the same time zone.
- OpenScape Business S multi-gateway networks have only been released within a country (same time zone, same CO access code).
- As a general rule, all OpenScape Business internetworks are configured using wizards. OpenScape Voice and OpenScape 4000 in the internetwork are configured per node in Expert mode.
- The Presence Manager (DSS server functionality = network-wide display of busy states at DSS keys + call pickup) is available in OpenScape Business networks.
- SIP-Q trunks with route 16 (last route) are used to configure homogeneous OpenScape Business communication systems via the **Networking Configuration** wizard. External SIP trunks (SIP interconnections) are used for networking OpenScape 4000, OpenScape Voice or other communication systems; the configuration is performed in Expert mode.
- If the system is configured as a slave or master using the **Networking Configuration** wizard, a check is performed to determine whether lines are assigned to "Networking" route. If not, 16 lines are automatically assigned to the "Networking" route. If the system is removed from the internetwork, these assignments are retained.
- In each node, only ONE voicemail system can be used. As a general rule, different voicemail systems are allowed in an OpenScape Business internetwork:
  - If the UC Suite is used, any other voicemail systems present in the internetwork must be disabled by the administrator.
  - A HiPath 3000 internetwork with different voicemail systems can be migrated 1:1 to OpenScape Business.
- For technical reasons, OpenScape Business X1 systems can not be set up as masters. Since a master system is required in each OpenScape Business network, at least one system must be larger than X1.

INFO: The relevant sales limits may differ from these details (and the following details in the individual scenarios). Please read the notes in the Sales Information.

21.6.2 Networking Multiple OpenScape Business X Systems

Up to 32 OpenScape Business X communication systems can be networked with each other.

Network Data



- With UC solution (UC Smart or UC Suite): Only closed numbering possible
- Without UC solution: Closed or open numbering possible
- Configuration via WBM (wizards) when using closed numbering
- UC Suite functionality based on UC Booster Server or UC Booster Card
- Up to 32 networked systems and 1500 users without UC solution
- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported

UC networking	Closed numbering	Open numbering
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Network-wide administration in Expert mode
Manager E	Network-wide administration for special tasks	Network-wide administration for special tasks
UC Suite Administration (for UC Booster Server and UC Booster Card)	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up networking with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).

  INFO: The station numbers may need to be adapted. An open numbering scheme is not implemented!

- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

Table 12: Setting up the Location Data for Node 1

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 13: Overview of Entries in the LCR for Node 1

Dial Plan		**Routing table**			**Dial Rule**		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C0049230266719-Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-Z						
Node 2 Stn.	0C66719-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table 14: Setting up the Location Data for Node 2

Node 2	
G.-Location Country	49
G.-Location Local Network	2302
G.-Location System	66719
International Prefix	00
National Prefix	0

Node 2		
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 15: Overview of Entries in the LCR for Node 2

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Procedure to Set up Networking:

1) Configure the basic installation for node 1 (master)
2) Configuring Networking for Node 1
3) Configure the basic installation for node 2 (slave)
4) Configuring Networking for Node 2
5) Verify the networking function for the master
6) Check routes and routing parameters (master)
7) Check routes and routing parameters (Trk. Grp. 16) (master)
8) Configure LCR for networking (master)
9) Check routes and routing parameters (Slave)
10) Configure LCR for networking (slave)

21.6.2.1 How to Configure the Basic Installation for Node 1 (Master)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important,

since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Basic Installation** wizard.
4) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
5) Enter the **Area Code** and **PABX number**.
6) Select the **Network Integration** check box.
7) In the **Node ID** field for OpenScape Business, enter a node ID that is unique in the internetwork (a "**1**" for the configuration example).
8) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
9) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
10) Enable the check box **Delete all station numbers** and click on **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

    NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

11) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
12) Now configure the IP clients.
13) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
14) Now configure the sending of e-mails.
15) Click on **Finish**.

21.6.2.2 How to Configure Networking for Node 1 (Master)

In the next step, the wizard is used to configure the networking.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.

3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Define the node type (**Master**).
6) Under **Node ID**, enter the appropriate node numbers of the associated OpenScape Business systems (in the configuration example, those of the slaves with node ID 2).
7) Under **IP Address**, enter the IP addresses of the associated OpenScape Business systems (in the configuration example, those of the slave with node ID 2).
8) Under **Name**, enter the appropriate type of the subsystem.
9) Enable the **Encryption Required** check box if required.

INFO: The encryption is based on SPE and does not apply to the applications!

NOTICE: Note that the encryption is not configured by simply enabling the check box. See Signaling and Payload Encryption (SPE) .

10) Click on **Finish**.

21.6.2.3 How to Configure the Basic Installation for Node 2 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.
6) In the **Node ID** field for OpenScape Business S, enter a node ID that is unique in the internetwork (a "**2**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.

9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the IP clients.
12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **Finish**.

21.6.2.4 How to Configure Networking for Node 2 (Slave)

In the next step, the wizard is used to configure the networking.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Under **Node type** , select the check box **This system is a SLAVE node**.
6) Enter the IP address of the master under **IP address**.

INFO: Note that this action cannot be undone after clicking **OK & Next**!

---

7) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
8) Click on **Finish**.

21.6.2.5 How to Verify the Networking Function for the Master

You can verify the status of the network in general and also the individual station numbers.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Network**.
2) The status bar shows the **Synchronization status** for the network. Green means that there are no networking problems; red indicates problems in the network.
3) Selecting the **Domain View** tab in the **Network** window shows all available nodes with the **Node ID**, **Name**, **System Type**, **Server Address**, **Registration Status** and **Availability Status**.
4) Selecting the **Phone Numbers** tab in the **Network** window opens a window with all the relevant details on the following:
   - **Call number**
   - **DID**
   - **Name**
   - **Port Type**
   - **Nodes**

21.6.2.6 How to Configure Routes and Routing Parameters (ISDN Trunk for the Master)

In the following steps, you will configure the routes for the networking of the master.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value `2302`.
8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `66758`.
9) Select the check box **Incoming PABX number** in the **Location number** field.
10) Click on **Apply** followed by **OK**.

21.6.2.7 How to Configure Routes and Routing Parameters (Trk. Grp. 16) (Master)

For route 64 (networking), the entry for the 2nd trunk code is mandatory for the master and slave and must be filled in. Route 16 is the default route for networking with OpenScape Business.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click on the last **Route** (**Route 16**).
4) In the **Change Route** window, enter a name for the network route in the **Route Name** field, e.g., `Networking`.
5) Do not enter anything for the **Seizure code**.
6) Enter a "0" under **CO code (2nd trunk code)** .
7) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
8) Click on **Apply** followed by **OK**.

21.6.2.8 How to Configure Least Cost Routing (LCR) for the Network (Master)

The default entries in index 32, 33 and 34 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to node 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.
4) Enter the following values in the free positions after the default values (35 to 37 in this case):

Dial Plan	Name	Dialed digits	Route table
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
35	Node 2 Inter	0C0049230266719-Z	16
36	Node 2 NAT	0C0230266719-Z	16
37	Node 2 Stn.	0C66719-Z	16

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for node 2.
   a) Under **Rule Name**, enter the value **Node 2**.
   b) Under **Dial rule format**, enter the value **D49230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.
7) Click on **Routing table** in the menu tree.
8) Click on routing table 16.
   a) Under **Route**, select the item **Networking**.
   b) Under **Dial Rule**, select the item **Node 2**.
   c) Under **min. COS**, select the item **15**.
   d) Under **Warning**, select the item **None**.
   e) Under **Dedicated Gateway**, select the item **Forced**.
   f) Under **GW Node ID**, select the item **2**.
   g) Click on **Apply** followed by **OK**.

21.6.2.9 How to Configure Routes and Routing Parameters (Slave)

In the following steps, you will configure the route and routing parameters for the networking of the slave.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the network route in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value `2302`.
8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `66719`.
9) Select the check box **Incoming PABX number** in the **Location number** field.
10) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
11) Click on **Apply** followed by **OK**.

21.6.2.10 How to Configure Least Cost Routing (LCR) for the Network (Slave)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to node 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **LCR**.

3) Click on **Dial Plan** in the menu tree.

4) Enter the following values in the free positions after the default values (35 to 37 in this case):

Dial Plan	Name	Dialed digits	Route table
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 1 Inter	0C0049230266758-Z	16
37	Node 1 NAT	0C00230266758-Z	16
38	Node 1 Stn.	0C66758-Z	16

5) Click on **Apply** followed by **OK**.

6) Click in the menu tree on **Dial Rule** for**Node 2**.

a) Under **Rule Name**, enter the value **Node 1**.
b) Under **Dial rule format**, enter the value **D49230266758E3A**.
c) Select **Corporate Network** as the **Network provider's method of access**.
d) Under **Type**, select the item **Country code**.
e) Click on **Apply** followed by **OK**.

7) Click on routing table 16.

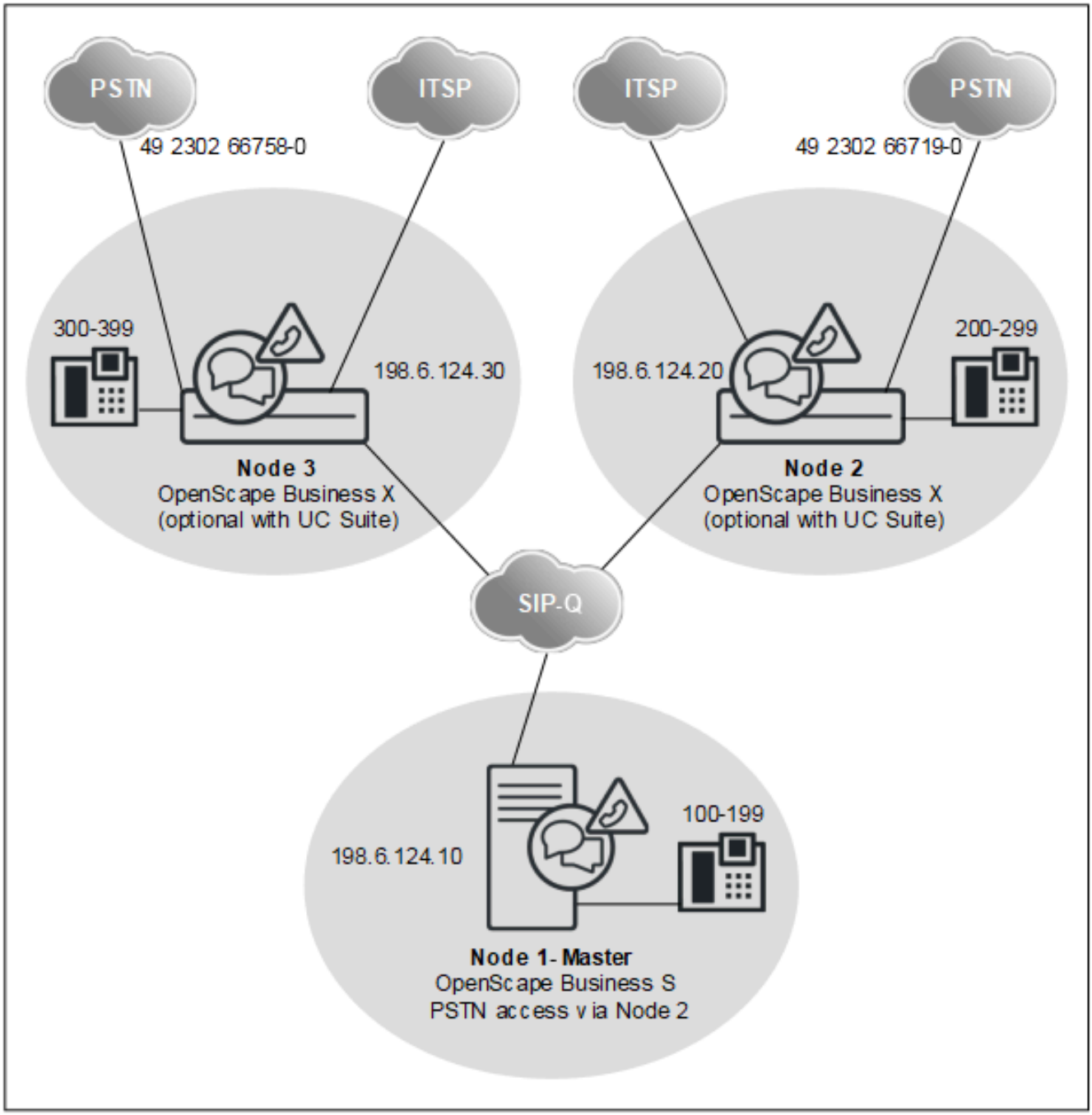
a) Under **Route**, select the item **Networking**.
b) Under **Dial Rule**, select the item **Node 1**.
c) Under **min. COS**, select the item **15**.
d) Under **Warning**, select the item **None**.
e) Under **Dedicated Gateway**, select the item **Forced**.
f) Under **GW Node ID**, select the item **2**.
g) Click on **Apply** followed by **OK**.

8) Click on **Routing table** in the menu tree.

21.6.3 Networking OpenScape Business X and OpenScape Business S (Single Gateway)

Up to 32 OpenScape Business X/S communication systems can be networked with each other. Multiple OpenScape Business S systems are allowed in an internetwork. Single Gateway means that all IP stations registered at OpenScape Business S only use ONE gateway to the PSTN or ITSP.

Network Data



- Closed numbering

- Network-wide voice and UC functionality with UC Suite configuration via WBM (wizards)
- The UC functionality is implemented either through the UC Booster Server or via the UC Booster Card
- Several OpenScape Business S in one internetwork are allowed.
- Up to 32 networked systems and 1500 users without UC solution
- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Not supported
Manager E	Network-wide administration for special tasks (not for OpenScape Business S)	Not supported
UC Suite Administration (for UC Booster Server and UC Booster Card)	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	Not supported

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	Not supported

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up networking with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once (e.g., the CO station numbers 49 2302 66758 100 and 49 2302 66719 100 have the same DID No. 100).
- The IP network has been configured, and all nodes can be mutually pinged successfully

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box.

In an internetwork in which the activation period is being used, the CLA of OpenScape Business S must always as be used as the central CLA!

Due to the different amounts of the upper limits, two different activation period files are required for OpenScape Business and OpenScape Business S. The activation period file for OpenScape Business S includes the OpenScape Business base in addition to the S base for networking scenarios.

In this scenario, whenever an OpenScape Business requests a license from a CLA of the OpenScape Business S during the activation period, the limits of the OpenScape Business S are used.

By contrast, if the CLA of the OpenScape Business were to be used instead, NO activation period would be granted to any requesting OpenScape Business S, since no basis for OpenScape Business S is included in this file.

Table 16: Setting up the Location Data for Node 1, OpenScape Business S

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
Trk. Grp 1	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 17: Overview of Entries in the LCR for Node 1

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Stn.	0C66719-2Z						
Node 3 Internat	0C0049230266758-3Z	Networking	Mandatory	3	D49230266758E3A	Corp. Network	International
Node 3 NAT	0C0230266758-3Z						
Node 3 Stn.	0C66758-3Z						
CO	0CZ	Networking	Mandatory	2	E1A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table 18: Setting up the Location Data for Node 2, OpenScape Business

Node 2		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 19: Overview of Entries in the LCR for Node 2

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266719-1Z	Networking	Mandatory	1	D49230266719E3A	Corp. Network	International
Node 1 NAT	0C0230266719-1Z						
Node 1 Stn.	0C66719-1Z						
Node 3 Internat	0C0049230266758-3Z	Networking	Mandatory	3	D49230266758E3A	Corp. Network	International
Node 3 NAT	0C0230266758-3Z						
Node 3 Stn.	0C66758-3Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Table 20: Setting up the Location Data for Node 3, OpenScape Business

Node 3		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 21: Overview of Entries in the LCR for Node 3

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266719-1Z	Networking	Mandatory	1	D49230266719E3A	Corp. Network	International
Node 1 NAT	0C0230266719-1Z						
Node 1 Stn.	0C66719-1Z						
Node 2 Internat	0C0049230266719-2Z	Networking	Mandatory	2	D49230266719E3A	Corp. Network	International
Node 2 NAT	0C0230266719-2Z						
Node 2 Stn.	0C66719-2Z						
CO	0CZ	ISDN	No		A	Main network supplier	Unknown
Various	-Z	Networking	No		A	Corp. Network	Unknown

Procedure to Set up Networking:

1) Configure the basic installation for node 1 (master)
2) Configuring Networking for Node 1
3) Configure the basic installation for node 2 (slave)
4) Configuring Networking for Node 2
5) Configure the basic installation for node 3 (slave)
6) Configure networking for node 3 (slave)
7) Verify the networking function for the master
8) Configure LCR for networking (node 1, master)
9) Configure LCR for networking (node 2)
10) Configure routes and routing parameters (node 3)
11) Configure routes and routing parameters (Trk. Grp. 16) (Node 3)
12) Configure LCR for networking (node 3)

21.6.3.1 How to Configure the Basic Installation for Node 1 (Master)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.
6) In the **Node ID** field, assign a unique node ID in the internetwork for OpenScape Business S. The node ID must be between "**1**" and "**100**" (select "**1**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Import the IP clients.
12) Now configure the Internet telephony.
13) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
14) Now configure the sending of e-mails.
15) Click on **OK & Next**.
16) Click on **Finish**.

21.6.3.2 How to Configure Networking for Node 1 (Master)

In the next step, the Network Configuration wizard is used to configure the networking for node 1 (master).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Define the node type (**Master**).

6) Under **Node ID**, enter the appropriate node numbers of the associated OpenScape Business systems (in the configuration example, those of the slaves with node ID 2).
7) Under **IP Address**, enter the IP addresses of the associated OpenScape Business systems (in the configuration example, those of the slaves with node IDs 2 and 3).
8) Select the check box **Gateway**.
9) Under **Name**, enter the type of system.
10) Under **Type**, enter the type of the subsystem.
11) Enable the **Encryption Required** check box if required.

INFO: The encryption is based on SPE and does not apply to the applications!

NOTICE: Note that the encryption is not configured by simply enabling the check box. See Signaling and Payload Encryption (SPE) .

12) Click on **Finish**.

21.6.3.3 How to Configure the Basic Installation for Node 2 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.
6) In the **Node ID** field for an OpenScape Business, enter a node ID that is unique in the internetwork (a "**2**" and a "**3**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.

9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the ISDN and analog stations.
12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **OK & Next**.
15) Click on **Finish**.

21.6.3.4 How to Configure Networking for Node 2 (Slave)

In the next step, the Network Configuration wizard is used to configure the networking of node 2.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Under **Node type** , select the check box **This system is a SLAVE node**.
6) **Enter die IP address of the MASTER node** (in the configuration example, the IP address of node 1).

INFO: Note that this action cannot be undone after clicking **OK & Next**!

---

7) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
8) Click on **Finish**.

21.6.3.5 How to Configure the Basic Installation for Node 3 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**. (identical to the assigned gateway system).
5) Select the **Network Integration** check box.
6) In the **Node ID** field for OpenScape Business, enter a node ID that is unique in the internetwork (a "**3**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the ISDN and analog stations.
12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **OK & Next**.
15) Click on **Finish**.

21.6.3.6 How to Verify the Networking Function for the Master

You can verify the status of the network in general and also the individual station numbers.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Network**.
2) The status bar shows the **Synchronization status** for the network. Green means that there are no networking problems; red indicates problems in the network.

3) Selecting the **Domain View** tab in the **Network** window shows all available nodes with the **Node ID**, **Name**, **System Type**, **Server Address**, **Registration Status** and **Availability Status**.
4) Selecting the **Phone Numbers** tab in the **Network** window opens a window with all the relevant details on the following:
   - **Call number**
   - **DID**
   - **Name**
   - **Port Type**
   - **Nodes**

21.6.3.7 Configure networking for node 3 (slave)

In the next step, the Network Configuration wizard is used to configure the networking for node 3.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Under **Node type** , select the check box **This system is a SLAVE node**.
6) **Enter die IP address of the MASTER node** (in the configuration example, the IP address of node 1).

INFO: Note that this action cannot be undone after clicking **OK & Next**!

---

7) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
8) Click on **Finish**.

21.6.3.8 How to Configure Least Cost Routing (LCR) for the Network (Node 3, Slave)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 1 and 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. The entries 36, 37 and 39 for interworking with node 1 (station numbers 100 > 199) and the entries 39, 40 and 41 for interworking with node 2 (station numbers 200 > 299) must be extended. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **LCR**.

3) Click on **Dial Plan** in the menu tree.

4) Enter the following values in the free positions after the default values (35 to 40 in this case):

Dial Plan	Name	Dialed digits	Route table
31	Appl-Suite	-371	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 1 Inter	0C0049230266719-1Z	16
37	Node 1 NAT	0C0230266719-1Z	16
38	Node 1 Stn.	0C66719-1Z	16
39	Node 2 Inter	0C0049230266719-2Z	17
40	Node 2 NAT	0C0230266719-2Z	17
41	Node 2 Stn.	0C66719-2Z	17

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for nodes 1 and 2.

a) Under **Rule Name**, enter the value **Node 1 + 2**.
b) Under **Dial rule format**, enter the value **D49230266719E3A**.
c) Select **Corporate Network** as the **Network provider's method of access**.
d) Under **Type**, select the item **Country code**.
e) Click on **Apply** followed by **OK**.

7) Click on **Routing table** in the menu tree to configure routing table 16 for networking and to assign it directly to node 1.

8) Click on routing table 16.

a) Under **Route**, select the item **Networking**.
b) Under **Dial Rule**, select the item **Nodes 1 + 2**.
c) Under **min. COS**, select the item **15**.
d) Under **Warning**, select the item **None**.
e) Under **Dedicated Gateway**, select the item **Forced**.
f) Under **GW Node ID**, select the item **1**.
g) Click on **Apply** followed by **OK**.

9) Click on **Routing table** in the menu tree to configure routing table 17 for networking and to assign it directly to node 2.

10) Click on routing table 17.

a) Under **Route**, select the item **Networking**.
b) Under **Dial Rule**, select the item **Nodes 1 + 2**.
c) Under **min. COS**, select the item **15**.
d) Under **Warning**, select the item **None**.
e) Under **Dedicated Gateway**, select the item **Forced**.
f) Under **GW Node ID**, select the item **2**.
g) Click on **Apply** followed by **OK**.

21.6.3.9 How to Configure LCR for Networking (Node 2)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 1 and 3. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. The entries 36, 37 and 38 for interworking with node 1 (station numbers 100 > 199) and the entries 39, 40 and 41 for interworking with node 3 (station numbers 300 > 399) must be extended. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **LCR**.

3) Click on **Dial Plan** in the menu tree.

4) Enter the following values in the free positions after the default values (35 to 40 in this case):

Dial Plan	Name	Dialed digits	Route table
31	Appl-Suite	-271	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 1 Inter	0C0049230266719-1Z	16
37	Node 1 NAT	0C0230266719-1Z	16
38	Node 1 Stn.	0C66719-1Z	16
39	Node 3 Inter	0C0049230266758-3Z	17
40	Node 3 NAT	0C0230266758-3Z	17
41	Node 3 Stn.	0C66758-3Z	17

5) Click on **Apply** followed by **OK**.

6) Click on **Routing table** in the menu tree.

7) In the menu tree, click on the associated **Dial Rule** for node 1.
   a) Under **Rule Name**, enter the value **Node 1**.
   b) Under **Dial rule format**, enter the value **D49230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.
8) Click on routing table 16 to configure it for node 1 networking.
   a) Under **Route**, select the item **Networking**.
   b) Under **Dial Rule**, select the item **Node 1**.
   c) Under **min. COS**, select the item **1**.
   d) Under **Warning**, select the item **None**.
   e) Under **Dedicated Gateway**, select the item **Forced**.
   f) Under **GW Node ID**, select the item **1**.
   g) Click on **Apply** followed by **OK**.
9) In the menu tree, click on the associated **Dial Rule** for node 3.
   a) Under **Rule Name**, enter the value **Node 3**.
   b) Under **Dial rule format**, enter the value **D49230266758E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.
10) Click on **Routing table** in the menu tree.
11) Click on routing table 17 to configure it for node 3 networking.
   a) Under **Route**, select the item **Networking**.
   b) Under **Dial Rule**, select the item **Node 3**.
   c) Under **min. COS**, select the item **1**.
   d) Under **Warning**, select the item **None**.
   e) Under **Dedicated Gateway**, select the item **Forced**.
   f) Under **GW Node ID**, select the item **3**.
   g) Click on **Apply** followed by **OK**.

21.6.3.10 How to Configure Routes and Routing Parameters (Node 1, Master)

In node 1, the settings for the CO trunk must be configured with respect to the location number, seizure code and routing parameters. The PABX number for defining the gateway location must be entered here. These entries are used for dialing from applications such as myPortal, for example.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.

5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value `2302`.
8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `66719`.
9) Select the check box **Incoming PABX number** in the **Location number** field.
10) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
11) Click on **Apply** followed by **OK**.

21.6.3.11 How to Configure Routes and Routing Parameters (Trk. Grp. 16, Node 1)

For route 64 (networking), the entry for the 2nd trunk code is mandatory for the master and slave and must be filled in.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click on the last **Route** (**Route 16**).
4) In the **Change Route** window, enter a name for the network route in the **Route Name** field, e.g., `Networking`.
5) Do not enter anything for the **Seizure code**.
6) Enter a "0" under **CO code (2nd trunk code)** .
7) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
8) Click on **Apply** followed by **OK**.

21.6.3.12 How to Configure Least Cost Routing (LCR) for the Network (Node 1)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 2 and 3. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.
4) Enter the following values in the free positions after the default values (35 to 40 in this case):

Dial Plan	Name	Dialed digits	Route table
16	Standard	0CZ	1
17	Standard	0C1Z	1
18	Standard	0CNZ	1
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 2 Inter	0C0049230266719-2Z	16
37	Node 2 NAT	0C0230266719-2Z	16
38	Node 2 Stn.	0C66719-2Z	16
39	Node 3 Inter	0C0049230266758-3Z	17
40	Node 3 NAT	0C0230266758-3Z	17
41	Node 3 Stn.	0C66758-3Z	17

5) Click on **Apply** followed by **OK**.
6) In the menu tree, click on the associated **Dial Rule** for node 2.
   a) Under **Rule Name**, enter the value **Node 2**.
   b) Under **Dial rule format**, enter the value **D49230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.
7) Click on **Routing table** in the menu tree.
8) Click on routing table 16 to configure it for node 2 networking.
   a) Under **Route**, select the item **Networking**.
   b) Under **Dial Rule**, select the item **Node 2**.
   c) Under **min. COS**, select the item **1**.
   d) Under **Warning**, select the item **None**.
   e) Under **Dedicated Gateway**, select the item **Forced**.
   f) Under **GW Node ID**, select the item **2**.
   g) Click on **Apply** followed by **OK**.
9) In the menu tree, click on the associated **Dial Rule** for node 3.
   a) Under **Rule Name**, enter the value **Node 3**.
   b) Under **Dial rule format**, enter the value **D49230266719E1A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.
10) Click on **Routing table** in the menu tree.

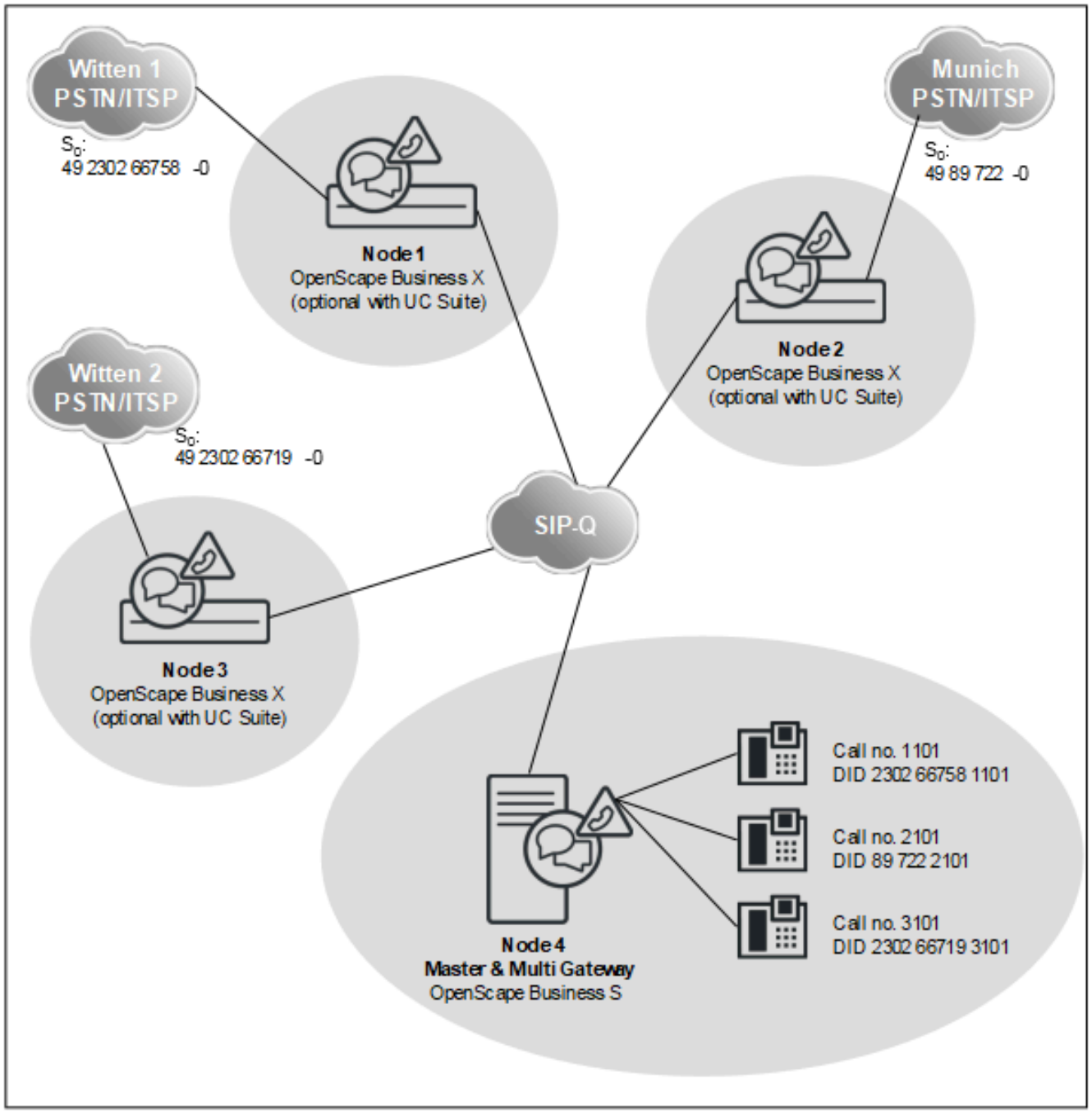
11) Click on routing table 17 to configure it for node 3 networking.
   a) Under **Route**, select the item **Networking**.
   b) Under **Dial Rule**, select the item **Node 3**.
   c) Under **min. COS**, select the item **1**.
   d) Under **Warning**, select the item **None**.
   e) Under **Dedicated Gateway**, select the item **Forced**.
   f) Under **GW Node ID**, select the item **3**.
   g) Click on **Apply** followed by **OK**.

12) Click on **Routing table** in the menu tree.

21.6.4 Networking OpenScape Business X and OpenScape Business S (Multi-Gateway)

Up to 32 OpenScape Business X and OpenScape Business S communication systems can be networked with one another. Multi-gateway means that every IP station registered at OpenScape Business S is assigned to exactly one specific gateway.

Network Data



- Closed numbering
- Network-wide voice and UC functionality with UC Suite configuration via WBM (wizards)
- The UC functionality is implemented either through the UC Booster Server or via the UC Booster Card
- Only one OpenScape Business S in the internetwork is allowed.
- All systems must have the same country code
- All systems must be located in the same time zone
- Only one CO access code (e.g., 0) must exist for the entire network.
- Up to 32 networked systems and 1500 users without UC solution

- Up to 8 networked systems and 1500 users with UC solution

Network-wide Features

UC networking	Closed numbering	Open numbering
Maximum number of nodes	8 with UC solution and 32 without UC solution	
Maximum number of stations in a single communication system	Depending on OpenScape Business X	
Maximum number of stations in the network	1500	

UC networking	Closed numbering	Open numbering
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported

Administration	Closed numbering	Open numbering
WBM	Network-wide administration using wizards	Not supported
Manager E	Network-wide administration for special tasks (not for OpenScape Business S)	Not supported
UC Suite Administration (for UC Booster Server and UC Booster Card	Network-wide administration using wizards	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	Not supported

Licensing	Closed numbering	Open numbering
Licensing structure	A networking license is required for each node	Not supported

Configuration

This configuration (with closed numbering and UC Suite) shows the steps required to set up a multi-gateway network with the help of an example.

Prerequisites:

- A network plan is available. The network plan was used to ensure that every internal call number in the internetwork is only used once for closed numbering. Different station number lengths are allowed. Only DID station numbers may occur more than once
- The IP network has been configured, and all nodes can be mutually pinged successfully
- All nodes have been upgraded to the same software version

Call forwarding across nodes: For incoming calls over IP trunks, which have already been forwarded, no further forwardings to the voicemail box are executed. This is because no unique assignment to the voicemail box can otherwise be made

If cross-node deputy rules (referral extensions) are required, this must be set up via the profiles of the OpenScape Business stations or ringing groups. The corresponding cross-node calls are not signaled as forwarded in this case, but as DSS (direct station selection) calls. Call forwardings of the deputy are therefore forwarded to the voicemail box

Table 22: Setting up the Location Data for Node 1

Node 1		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66758
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 23: Overview of Entries in the LCR for Node 1

Dial Plan		**Routing table**			**Dial Rule**		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 3 Internat	0C0049230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 3 Stn.	0C66719-Z						
Node 4 Internat	0C0049230266758-Z	Networking	NO		D230266758E3A	Corp. Network	National
Node 4 NAT	0C0230266758-Z						
Node 4 Stn.	0C66758-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Table 24: Setting up the Location Data for Node 2

Node 2		
G.-Location Country		49
G.-Location Local Network		89
G.-Location System		722
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 2 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 25: Overview of Entries in the LCR for Node 2

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D492302667E3A	Corp. Network	International

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
Node 3 Internat	0C0049230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International
Node 3 NAT	0C0230266719-Z						
Node 3 Stn.	0C66719-Z						
Node 4 Internat	0C004989722-Z	Networking	NO		D89722E3A	Corp. Network	National
Node 4 NAT	0C089722-Z						
Node 4 Stn.	0C722-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Table 26: Setting up the Location Data for Node 3

Node 3		
G.-Location Country		49
G.-Location Local Network		2302
G.-Location System		66719
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 3 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 27: Overview of Entries in the LCR for Node 3

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 1 Stn.	0C66758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 2 Stn.	0C722-Z						
Node 4 Internat	0C004989230266719-Z	Networking	No		D230266719E3A	Corp. Network	National
Node 4 NAT	0C0230266719-Z						
Node 4 Stn.	0C66719-Z						
Various	-Z	Networking	No		BA	Corp. Network	Unknown
CO International	0C0049-Z	ISDN	No		D0E3A	Main network supplier	Unknown
CO	0CZ	ISDN	No		A	Main network supplier	Unknown

Setting up the Location Data for Node 4: Associate location data with a dummy CO trunk (Trk. Grp. 1) incl. CO access code = 0 and Type = CO, since node 4 has no direct connection to a Central Office.

Table 28: Node 4, dummy CO trunk

Node 4	
G.-Location Country	49
G.-Location Local Network	
G.-Location System	
International Prefix	00
National Prefix	0
Routes	

Node 4		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	Unknown	Int/DID
ISDN	(No change in entry)	DID

The station numbers of all stations outside node 1 are automatically entered in the routing tables. This includes the internal station numbers as well as the DID station numbers, which differ from the respective internal station numbers.

Table 29: Node 4, Networking Route

Node 4		
G.-Location Country		
G.-Location Local Network		
G.-Location System		
International Prefix		00
National Prefix		0
Routes		
ISDN	Trunk code	0
Networking	2nd trunk code	0
Routing parameters		
Route	No. and type, outgoing	RNR type
Networking	National	Int/DID
ISDN	(No change in entry)	DID

Table 30: Overview of Entries in the LCR for Node 4

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 1 Internat	0C0049230266758-Z	Networking	Mandatory	1	D49230266758E3A	Corp. Network	International
Node 1 NAT	0C0230266758-Z						
Node 2 Internat	0C004989722-Z	Networking	Mandatory	2	D4989722E3A	Corp. Network	International
Node 2 NAT	0C089722-Z						
Node 3 Internat	0C004989230266719-Z	Networking	Mandatory	3	D49230266719E3A	Corp. Network	International

Dial Plan		Routing table			Dial Rule		
Name	**Dialed digits**	**Route**	**Dedicated Gateway**	**Gateway ID**	**Dial Rule**	**Procedure**	**Type**
Node 3 NAT	0C0230266719-Z						
Various	-Z	Networking	NO		A	Corp. Network	Unknown
CO	0CZ	Networking	MULTI-GATEWAY	1	E1A	Main network supplier	Unknown

Procedure to Set up Networking:

1) Configure the basic installation for node 4 (master)
2) Configure networking for node 4 (master)
3) Configure the basic installation for node 1 (slave)
4) Configure networking for node 1 (slave)
5) Configure the basic installation for node 2 (slave)
6) Configure networking for node 2 (slave)
7) Configure the basic installation for node 3 (slave)
8) Configure networking for node 3 (slave)
9) Verify the networking function for the master
10) Configure a multi-gateway for node 4 (master)
11) Configure routes and routing parameters (node 1, slave)
12) Configure LCR for networking (node 1, slave)
13) Configure routes and routing parameters (node 2, slave)
14) Configure LCR for networking (node 2, slave)
15) Configure routes and routing parameters (node 3, slave)
16) Configure LCR for networking (node 3, slave)
17) Configure routes and routing parameters (node 4, master)
18) Configure LCR for networking (node 4, master)

21.6.4.1 How to Configure the Basic Installation for Node 4 (OpenScape Business S, Master)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Do not make any entries in the **Area Code** and **PABX number** fields!

5) Select the **Network Integration** check box.
6) In the **Node ID** field, assign a unique node ID in the internetwork for OpenScape Business S. The node ID must be between "**1**" and "**100**" (a "**1**" was assigned for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the IP clients.
12) Configure the IP clients.
13) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
14) Now configure the sending of e-mails.
15) Click on **Finish**.

21.6.4.2 How to Configure the Networking for Node 4 (Master)

In the next step, the Network Configuration wizard is used to configure the networking for node 3.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Select the **This system is the MASTER node** check box.
6) Under **Node ID**, enter the corresponding node numbers of the associated OpenScape Business systems (in the configuration example, those of the slaves with node IDs 1, 2 and 3).
7) Under **IP Address**, enter the IP addresses of the associated OpenScape Business systems (in the configuration example, those of the slaves with node IDs 1, 2 and 3).
8) Select the check box **Gateway**.
9) Under **Name**, enter the type of system (for example: Slave 1).

10) Under **Type**, enter the type of the subsystem.
11) Enable the **Encryption Required** check box if required.

INFO: The encryption is based on SPE and does not apply to the applications!

NOTICE: Note that the encryption is not configured by simply enabling the check box. See Signaling and Payload Encryption (SPE) .

12) Click on **Finish**.

21.6.4.3 How to Configure the Basic Installation for Node 1 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.
6) In the **Node ID** field for OpenScape Business S, enter a node ID that is unique in the internetwork (a "**1**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the ISDN and analog stations.

12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **Finish**.

21.6.4.4 How to Configure Networking for Node 1 (Slave)

In the next step, the wizard is used to configure the networking.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) **Enter the IP address of the MASTER node** (The OpenScape Business is configured as a slave node and the corresponding IP address of the master node (the OpenScape Business S) is entered. The master and multi-gateway are always assigned to the same system, which is OpenScape Business S in the configuration example).

   INFO: Note that this action cannot be undone after clicking **OK & Next**!

6) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
7) Click on **Finish**.

21.6.4.5 How to Configure the Basic Installation for Node 2 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.

6) In the **Node ID** field for OpenScape Business S, enter a node ID that is unique in the internetwork (a "**2**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

---

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the ISDN and analog stations.
12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **Finish**.

21.6.4.6 How to Configure Networking for Node 2 (Slave)

In the next step, the Network Configuration wizard is used to configure the networking of node 2.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Under **Node type** , select the check box **This system is a SLAVE node**.
6) **Enter the IP address of the MASTER node** (The OpenScape Business is configured as a slave node and the corresponding IP address of the master node (the OpenScape Business S) is entered. The master and multi-gateway are always assigned to the same system, which is OpenScape Business S in the configuration example).

INFO: Note that this action cannot be undone after clicking **OK & Next**!

---

7) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
8) Click on **Finish**.

21.6.4.7 How to Configure the Basic Installation for Node 3 (Slave)

For integration in an internetwork, the country code and a node ID must be assigned. The internal station numbers must be uniquely configured throughout the network. The entry of the national and local station numbers is important, since this station number is set in the Trk. Grp. 1 ISDN trunk and used as the location number for normalization.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Basic Installation**.
3) In the **Country Code** field, enter the country code prefix, e.g., 49 for Germany.
4) Enter the **Area Code** and **PABX number**.
5) Select the **Network Integration** check box.
6) In the **Node ID** field for OpenScape Business, enter a node ID that is unique in the internetwork (a "**3**" for the configuration example).
7) Click on **Execute function**. You are taken to the **Central Functions for Stations** window.
8) Since all internal station numbers must be unique in a network, the standard station numbers must be deleted. Enable the **Delete all station call numbers** radio button.
9) Enable the check box **Delete all station numbers** and click **OK & Next**. You are taken to the **Change preconfigured call and functional numbers** window.

   NOTICE: The function codes must be unique in the internetwork. Duplicate station numbers are not allowed!

10) Adapt the preconfigured station numbers to the station numbers in the network and click **OK & Next**. You can optionally adapt the station numbers manually via the wizard or import a CSV file with the appropriately prepared station numbers.
11) Now configure the ISDN and analog stations.
12) Edit the settings for a Meet-Me conference. You must enter a code that is unique in the internetwork.
13) Now configure the sending of e-mails.
14) Click on **Finish**.

21.6.4.8 How to Configure Networking for Node 3 (Slave)

In the next step, the Network Configuration wizard is used to configure the networking for node 3.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Basic Installation**.
3) Click on **Edit** to start the **Networking Configuration** wizard.
4) Select the **Network with OSBiz X / S OSBiz S** setting.
5) Under **Node type** , select the check box **This system is a SLAVE node**.
6) **Enter the IP address of the MASTER node** (The OpenScape Business is configured as a slave node and the corresponding IP address of the master node (the OpenScape Business S) is entered. The master and multi-location are always assigned to the same system, which is OpenScape Business S in the configuration example).

   INFO: Note that this action cannot be undone after clicking **OK & Next**!

7) The **Registration Status** displays **Status successful** (or a corresponding error message). This completes the wizard.
8) Click on **Finish**.

21.6.4.9 How to Verify the Networking Function for the Master

You can verify the status of the network in general and also the individual station numbers.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Network**.
2) The status bar shows the **Synchronization status** for the network. Green means that there are no networking problems; red indicates problems in the network.
3) Selecting the **Domain View** tab in the **Network** window shows all available nodes with the **Node ID**, **Name**, **System Type**, **Server Address**, **Registration Status** and **Availability Status**.
4) Selecting the **Phone Numbers** tab in the **Network** window opens a window with all the relevant details on the following:
   - **Call number**
   - **DID**
   - **Name**
   - **Port Type**
   - **Nodes**

21.6.4.10 How to Configure a Multi-Gateway for Node 4 (Master)

The setup of the internetwork as a multi-gateway network is performed at the master node.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Networking Configuration**.
3) Under **Network Configuration**, select the setting **Multi-Location setup**. The assignment of stations to the location is specified in the **Multi-Location setup** window. The assignment of the call numbers to the node ID is used for the outbound trunk seizure in the assigned location nodes, for example.
4) Enter the following assignments under **Multi-Location setup** for the configuration example (all telephones are registered at OpenScape Business S):

Phone number	Name	Node ID
1101	1101KN1	1-Slave Witten1
1102	1102KN1	1-Slave Witten1
1103	1103KN1	1-Slave Witten1
2101	2101KN2	2-Slave Munich
2102	2102KN2	2-Slave Munich
2103	2103KN2	2-Slave Munich
3101	3101KN3	3-Slave Witten 2
3102	3102KN3	3-Slave Witten 2
3103	3103KN3	3-Slave Witten 2

5) Click on **Finish**.

21.6.4.11 How to Configure Routes and Routing Parameters (Node 1, Slave)

In the following steps, you will configure the route and routing parameters for the networking of the slave.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value `2302`.

8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `66758`.
9) Select the check box **Incoming PABX number** in the **Location number** field.
10) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
11) Click on **Apply** followed by **OK**.

21.6.4.12 How to Configure Least Cost Routing (LCR) for the Network (Node 1, Slave)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in the "international, national and station" formats for calls to nodes 2 and 3 and to the multi-gateway node 4. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.
4) Enter the following values in the free positions after the default values (36 to 43 in this case):

Dial Plan	Name	Dialed digits	Route table
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 2 Inter	0C004989722-Z	16
37	Node 2 NAT	0C089722-Z	16
38	Node 3 Inter	0C0049230266719-Z	17
39	Node 3 NAT	0C0230266719-Z	17
40	Node 3 Stn.	0C66719-Z	17
41	Node 4 Inter	0C0049230266758-Z	18
42	Node 4 NAT	0C0230266758-Z	18
43	Node 4 Stn.	0C66758-Z	18
44			-

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for node 2.
   a) Under **Rule Name**, enter the value **Node 2**.
   b) Under **Dial rule format**, enter the value **D4989722E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.

7) Click on **Routing table** in the menu tree to configure routing table 16 for networking and to directly assign it to node 2.
   a) Click on routing table 16.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 2**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **2**.
   h) Click on **Apply** followed by **OK**.

8) In the menu tree, click on the associated **Dial Rule** for node 3.
   a) Under **Rule Name**, enter the value **Node 3**.
   b) Under **Dial rule format**, enter the value **D49230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.

9) Click on **Routing table** in the menu tree to configure routing table 17 for networking and to directly assign it to node 3.
   a) Click on routing table 17.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 3**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **3**.
   h) Click on **Apply** followed by **OK**.

10) In the menu tree, click on the associated **Dial Rule** for node 4.
   a) Under **Rule Name**, enter the value **Node 4**.
   b) Under **Dial rule format**, enter the value **D230266758E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **National**.
   e) Click on **Apply** followed by **OK**.

11) Click on **Routing table** in the menu tree to configure routing table 18 for networking and to directly assign it to node 4.
   a) Click on routing table 18.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 4**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Click on **Apply** followed by **OK**.

21.6.4.13 How to Configure Routes and Routing Parameters (Node 2, Slave)

In the following steps, you will configure the route and routing parameters for the networking of the slave.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value 89.
8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `722`.
9) Select the check box **Incoming PABX number** in the **Location number** field.
10) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
11) Click on **Apply** followed by **OK**.

21.6.4.14 How to Configure Least Cost Routing (LCR) for the Network (Node 2, Slave)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 1 and 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. The entries 36, 37 and 38 for interworking with node 1 (station numbers 100 > 199) and the entries 39, 40 and 41 for interworking with node 3 (station numbers 300 > 399) must be extended. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.

4) Enter the following values in the free positions after the default values (36 to 43 in this case):

Dial Plan	Name	Dialed digits	Route table
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 1 Inter	0C0049230266758-Z	16
37	Node 1 NAT	0C0230266758-Z	16
38	Node 3 Inter	0C0049230266719-Z	17
39	Node 3 NAT	0C0230266719-Z	17
40	Node 3 Stn.	0C66719-Z	17
41	Node 4 Inter	0C004989722-Z	18
42	Node 4 NAT	0C089722-Z	18
43	Node 4 Stn.	0C722-Z	18
44			-

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for node 1.

a) Under **Rule Name**, enter the value **Node 1**.
b) Under **Dial rule format**, enter the value **D49230266758E3A**.
c) Select **Corporate Network** as the **Network provider's method of access**.
d) Under **Type**, select the item **Country code**.
e) Click on **Apply** followed by **OK**.

7) Click on **Routing table** in the menu tree to configure routing table 16 for networking and to assign it directly to node 1.

a) Click on routing table 16.
b) Under **Route**, select the item **Networking**.
c) Under **Dial Rule**, select the item **Node 1**.
d) Under **min. COS**, select the item **15**.
e) Under **Warning**, select the item **None**.
f) Under **Dedicated Gateway**, select the item **Forced**.
g) Under **GW Node ID**, select the item **1**.
h) Click on **Apply** followed by **OK**.

8) In the menu tree, click on the associated **Dial Rule** for node 3.

a) Under **Rule Name**, enter the value **Node 3**.
b) Under **Dial rule format**, enter the value **D49230266719E3A**.
c) Select **Corporate Network** as the **Network provider's method of access**.
d) Under **Type**, select the item **Country code**.
e) Click on **Apply** followed by **OK**.

9) Click on **Routing table** in the menu tree to configure routing table 17 for networking and to directly assign it to node 3.
   a) Click on routing table 17.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 3 Direct**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **3**.
   h) Click on **Apply** followed by **OK**.
10) In the menu tree, click on the associated **Dial Rule** for node 4.
   a) Under **Rule Name**, enter the value **Node 4**.
   b) Under **Dial rule format**, enter the value **D89722E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Local area code**.
   e) Click on **Apply** followed by **OK**.
11) Click on **Routing table** in the menu tree to configure routing table 18 for networking and to directly assign it to node 4.
   a) Click on routing table 18.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 4**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Click on **Apply** followed by **OK**.

21.6.4.15 How to Configure Routes and Routing Parameters (Node 3, Slave)

In the following steps, you will configure the route and routing parameters for the networking of the slave.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Under **Incoming PABX number**, in the **Local area code** field, enter the value `2302`.
8) Under **Incoming PABX number**, in the **PABX number** field, enter the value `66719`.

9) Select the check box **Incoming PABX number** in the **Location number** field.
10) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
11) Click on **Apply** followed by **OK**.

21.6.4.16 How to Configure Least Cost Routing (LCR) for the Network (Node 3, Slave)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 1 and 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.
4) Enter the following values:

Dial Plan	Name	Dialed digits	Route table
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	14
36	Node 1 Inter	0C0049230266758-Z	16
37	Node 1 NAT	0C00230266758-Z	16
38	Node 1 Stn.	0C66758-Z	16
39	Node 2 Inter	0C004989722-Z	17
40	Node 2 NAT	0C0089722-Z	17
41	Node 4 Inter	0C0049230266719-Z	18
42	Node 4 NAT	0C0230266719-Z	18
43	Node 4 Stn.	0C66719-Z	18
44			-

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for node 1.
   a) Under **Rule Name**, enter the value **Node 1**.
   b) Under **Dial rule format**, enter the value **D49230266758E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.

7) Click on **Routing table** in the menu tree to configure routing table 16 for networking and to assign it directly to node 1.
   a) Click on routing table 16.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 1**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **1**.
   h) Click on **Apply** followed by **OK**.

8) In the menu tree, click on the associated **Dial Rule** for node 2.
   a) Under **Rule Name**, enter the value **Node 2**.
   b) Under **Dial rule format**, enter the value **D4989722E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.

9) Click on **Routing table** in the menu tree to configure routing table 17 for networking and to assign it directly to node 2.
   a) Click on routing table 17.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 2**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **2**.
   h) Click on **Apply** followed by **OK**.

10) In the menu tree, click on the associated **Dial Rule** for node 4.
   a) Under **Rule Name**, enter the value **Node 4**.
   b) Under **Dial rule format**, enter the value **D230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Local area code**
   e) Click on **Apply** followed by **OK**.

11) Click on **Routing table** in the menu tree to configure routing table 18 for networking and to directly assign it to node 4.
   a) Click on routing table 18.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 4**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Click on **Apply** followed by **OK**.

21.6.4.17 How to Configure Routes and Routing Parameters (Node 4, Master)

In the following steps, you will configure the route and routing parameters for the networking of the slave.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **Trunks/Routing**.
3) In the menu tree, click **Route**.
4) In the **Change Route** window, enter a name for the CO trunk in the **Route Name** field, e.g., `Route 1`.
5) Under **Seizure code**, enter `0`.
6) Under **Incoming PABX number** , in the **Country code** field, enter the value `49`.
7) Do not make any entries in the **Local area code** and PABX number fields.
8) Select the check box **Incoming PABX number** in the **Location number** field.
9) The default settings for the routing parameters (No. and type, outgoing, Call number type) can be used.
10) Click on **Apply** followed by **OK**.

21.6.4.18 How to Configure Least Cost Routing (LCR) for the Network (Node 4, Master)

The default entries in index 32, 33, 34 and 35 in the LCR dial plan must be extended with further entries to enable the dialing of station numbers in "international, national and station" formats for calls to nodes 1 and 2. "International" and "National" are always needed. "Local" is only needed for partner nodes that are in the same local network. These entries are used for dialing from applications (e.g., myPortal for Desktop).

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click on **Dial Plan** in the menu tree.
4) Enter the following values in the free positions after the default values (36 to 43 in this case):

Dial Plan	Name	Dialed digits	Route table
1	Calling for Help	0C112	19
2	Calling for Help	0C110	19
3	Teleworking	0C0137Z	19

Dial Plan	Name	Dialed digits	Route table
4	Televoting	0C0138Z	19
5	Premium Services	0C0900Z	19
6	Information service	0C118Z	19
7	Special phone number	0C116116	19
16	Standard	0CZ	19
17	Standard	0C1Z	19
18	Standard	0CNZ	19
31	Appl-Suite	-471	12
32	Standard	88CZ	1
33	IP Network	-Z	13
34	CO Internat	0C0049-Z	15
36	Node 1 Inter	0C0049230266758-Z	16
37	Node 1 NAT	0C0230266758-Z	16
38	Node 1 Stn.	0C66758-Z	16
39	Node 2 Inter	0C004989722-Z	17
40	Node 2 NAT	0C089722-Z	17
41	Node 3 Inter	0C0049230266719-Z	18
42	Node 3 NAT	0C0230266719-Z	18
43	Node 3 Stn.	0C66719-Z	18
44			-

5) Click on **Apply** followed by **OK**.

6) In the menu tree, click on the associated **Dial Rule** for node 1.

a) Under **Rule Name**, enter the value **Node 1**.
b) Under **Dial rule format**, enter the value **D49230266758E3A**.
c) Select **Corporate Network** as the **Network provider's method of access**.
d) Under **Type**, select the item **Country code**.
e) Click on **Apply** followed by **OK**.

7) Click on **Routing table** in the menu tree to configure routing table 16 for networking and to assign it directly to node 1.

a) Click on routing table 16.
b) Under **Route**, select the item **Networking**.
c) Under **Dial Rule**, select the item **Node 1**.
d) Under **min. COS**, select the item **15**.
e) Under **Warning**, select the item **None**.
f) Under **Dedicated Gateway**, select the item **Forced**.
g) Under **GW Node ID**, select the item **1**.
h) Click on **Apply** followed by **OK**.

8) In the menu tree, click on the associated **Dial Rule** for node 2.
   a) Under **Rule Name**, enter the value **Node 2**.
   b) Under **Dial rule format**, enter the value **D4989722E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**.
   e) Click on **Apply** followed by **OK**.

9) Click on **Routing table** in the menu tree to configure routing table 17 for networking and to assign it directly to node 2.
   a) Click on routing table 17.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 2**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **2**.
   h) Click on **Apply** followed by **OK**.

10) In the menu tree, click on the associated **Dial Rule** for node 3.
   a) Under **Rule Name**, enter the value **Node 3**.
   b) Under **Dial rule format**, enter the value **D230266719E3A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Country code**
   e) Click on **Apply** followed by **OK**.

11) Click on **Routing table** in the menu tree to configure routing table 18 for networking and to directly assign it to node 3.
   a) Click on routing table 18.
   b) Under **Route**, select the item **Networking**.
   c) Under **Dial Rule**, select the item **Node 3**.
   d) Under **min. COS**, select the item **15**.
   e) Under **Warning**, select the item **None**.
   f) Under **Dedicated Gateway**, select the item **Forced**.
   g) Under **GW Node ID**, select the item **3**.
   h) Click on **Apply** followed by **OK**.

12) In the menu tree, click on the associated **Dial Rule** for trunk calls. This is the predefined dial rule "Gateway Call".
   a) Under **Rule Name**, enter the value **Gateway Call**.
   b) Under **Dial rule format**, enter the value **E1A**.
   c) Select **Corporate Network** as the **Network provider's method of access**.
   d) Under **Type**, select the item **Unknown**.
   e) Click on **Apply** followed by **OK**.

13) Click on **Routing table** in the menu tree to configure the route table 19 for the breakout of the slave. Using the multi-gateway entry, the association of the subscriber to the node is determined, and the breakout occurs at that node.

14) Click on routing table 19.

a) Under **Route**, select the item **Networking**.
b) Under **Dial Rule**, select the item **Gateway Call**.
c) Under **min. COS**, select the item **15**.
d) Under **Warning**, select the item **None**.
e) Under **Dedicated Gateway**, select the item **Multi-Gateway**.
f) Under **GW Node ID**, select the item **1**.
g) Click on **Apply** followed by **OK**.

21.6.5 Networking OpenScape Business in Hosting Environments

In an environment with multiple locations (hosting environment), each site can be assigned a route, and each route can be assigned an ITSP registration. A maximum of 8 ITSP registrations can be managed. One registration per ITSP is possible or even multiple registrations at one ITSP. Each ITSP registration can be assigned an area code, and multiple subscribers can then be assigned to it. The connection between the subscribers at the different sites and the communication system occurs via a VPN or MPLS. If the sites are located in different countries, a separate OpenScape Business S must be used for each country (Scenario 1a). If all sites are located within one country, a single OpenScape Business S can be used (Scenario 1b).

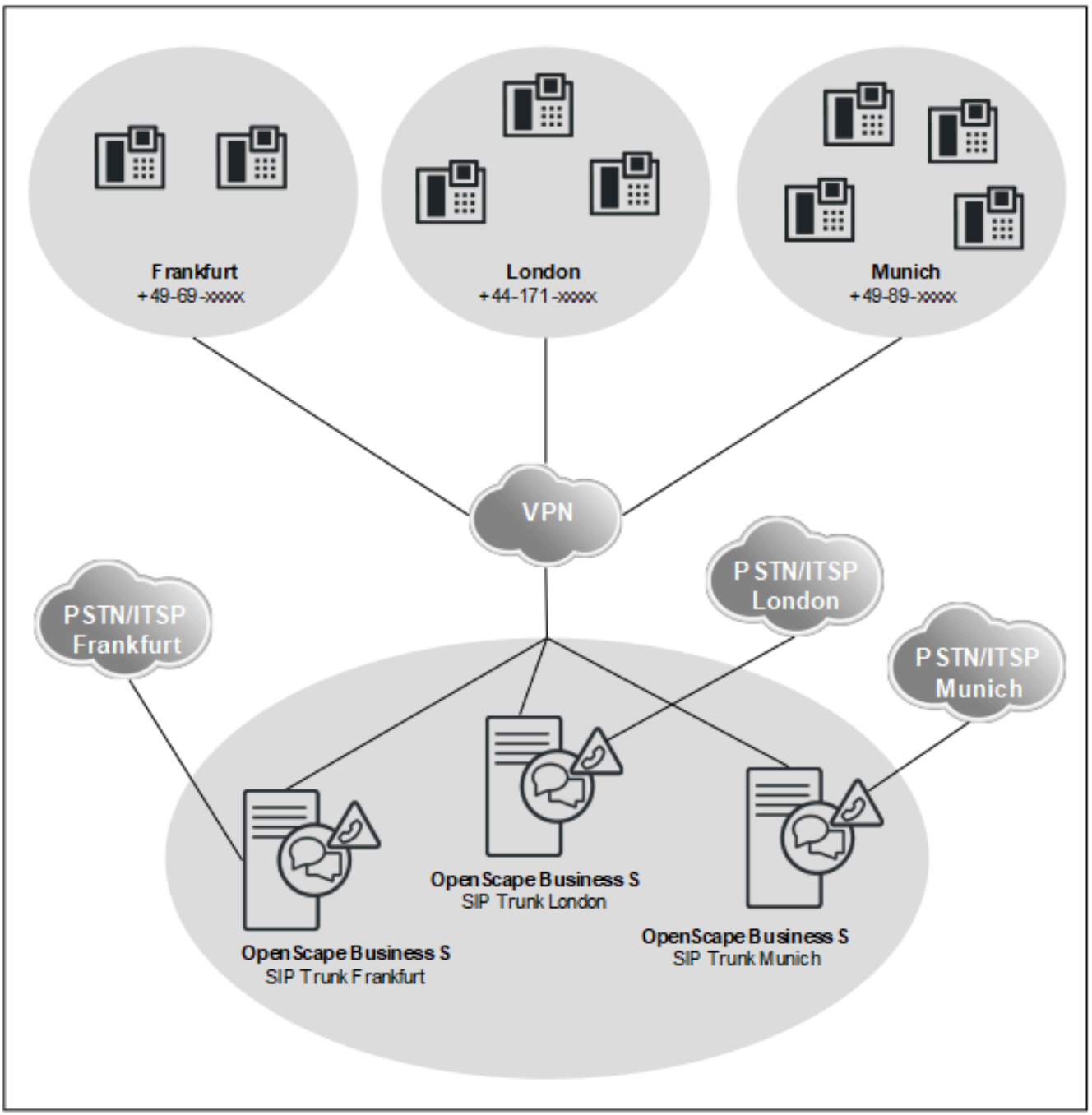
Both scenarios can also be implemented with the OpenScape Business X hardware models (e.g., for smaller configurations). The TDM components can be additionally used at one site.

The following hosting scenarios are described here in general. The following variations can be implemented:

- Use of OpenScape Business S and OpenScape Business X in the Data Center of the customer or at the hoster
- OpenScape Business S on dedicated server hardware or virtualized
- This requires a VPN or MPLS infrastructure, especially for multiple customer sites (no site-specific NAT router for Internet access)
- Up to 8 ITSP per system and country, MSN or DID provider
- Up to 8 site area codes per system and country, assigned to up to 8 customer sites (multi-site)
- Multi-site scenarios combined with classic networking (Voice and UC)
- Multi-site with more than 8 locations feasible in networks (multi-site networked n times)
- Transnational multi-site (multi-site networked n times) feasible in networks
- Networking scenarios with ISDN gateways fully integratable
- The technical prerequisite is the ability to use DID phone numbers for both ISDN providers as well as SIP providers.

Scenario a: Hosting with an OpenScape Business S per Site

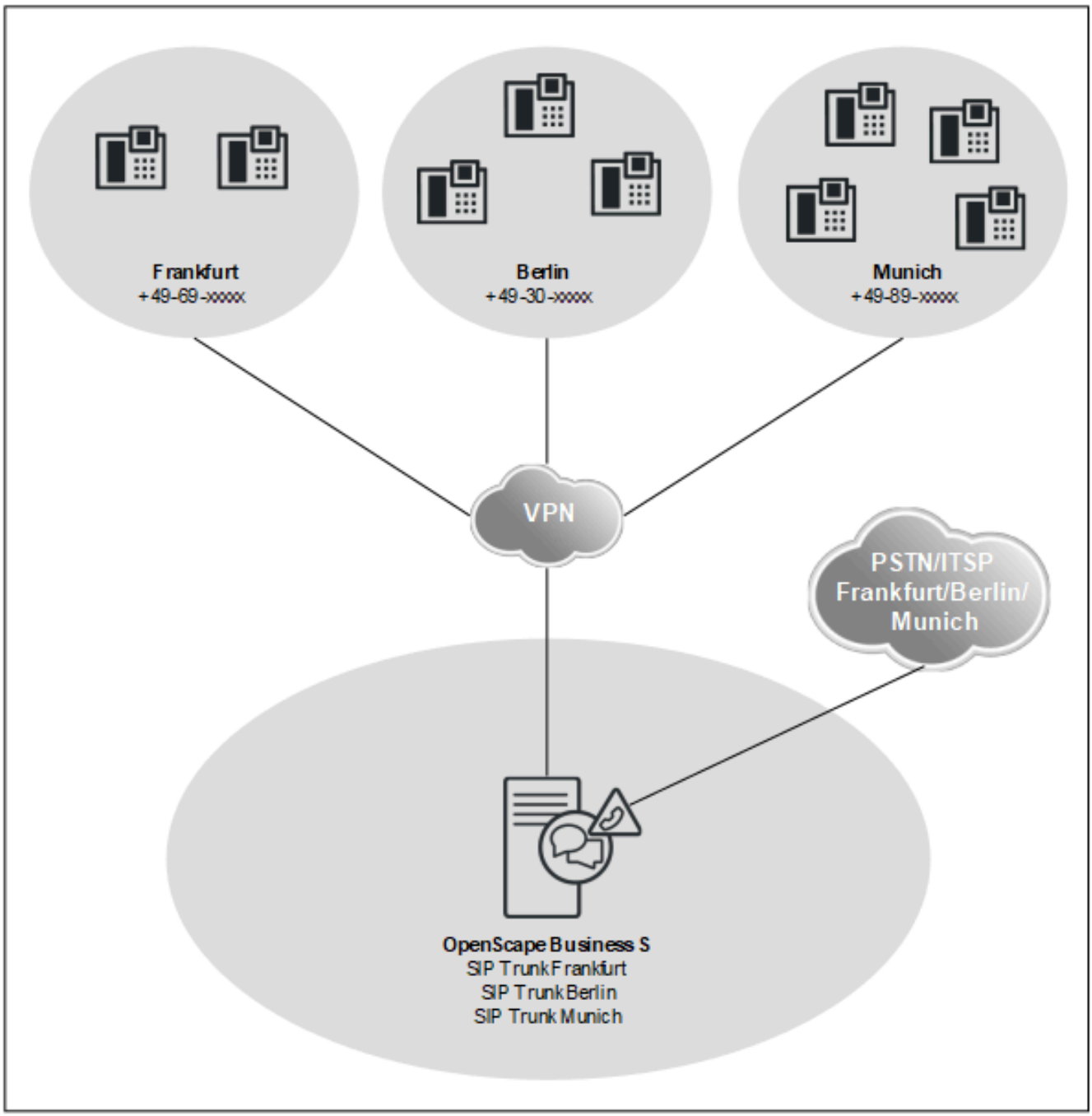
Network Data



- A customer within a VPN or MPLS.
- One OpenScape Business S per site.
- The sites may be distributed within a country or across multiple countries.
- Up to 1000 users and 180 SIP trunks per OpenScape Business S.
- OpenScape Business networking is optional, up to a total of 1500 users. Larger configurations are possible within the framework of project-specific releases.

Scenario b: Hosting with OpenScape Business S for Multiple Sites

Network Data



- A customer within a VPN or MPLS.
- One OpenScape Business S for all sites.
- All sites located within only one country.
- Up to 8 sites with different site prefixes
- Up to 8 SIP providers per OpenScape Business S.
- One SIP provider per site.
- Up to 1000 users and 180 SIP trunks.

- OpenScape Business networking with multiple OpenScape Business S within a VPN is optional (OS Biz S 1 in country 1, OS Biz S 2 in country 2, etc.), up to a total of 1500 users. Larger configurations are possible within the framework of project-specific releases.
- A configuration example can be found at the Unify Experts wiki on the Internet under *ITSP Configuration Guide*,

21.6.6 Networking OpenScape Business X and OpenScape 4000

Networking of OpenScape Business X with OpenScape 4000 can take two different forms. First, with direct addressing between the OpenScape Business nodes (Scenario 4a), and second, with the routing of all connections via OpenScape 4000 (Scenario 4b).

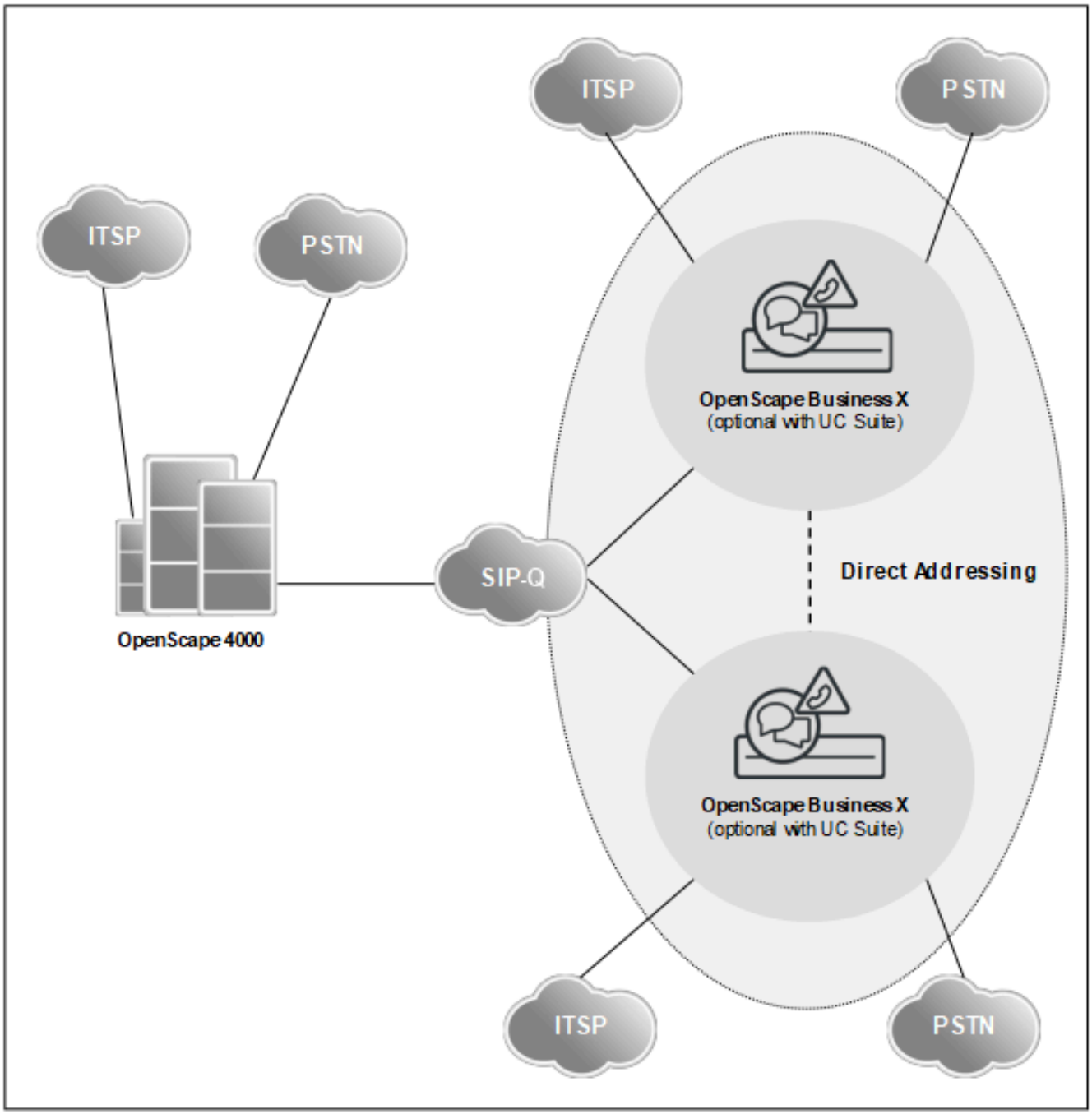
NOTICE: A configuration example for networking with OpenScape Voice can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Scenario a: Internet work with OpenScape 4000 and Direct Addressing Between the OpenScape Business X Nodes

Network Data

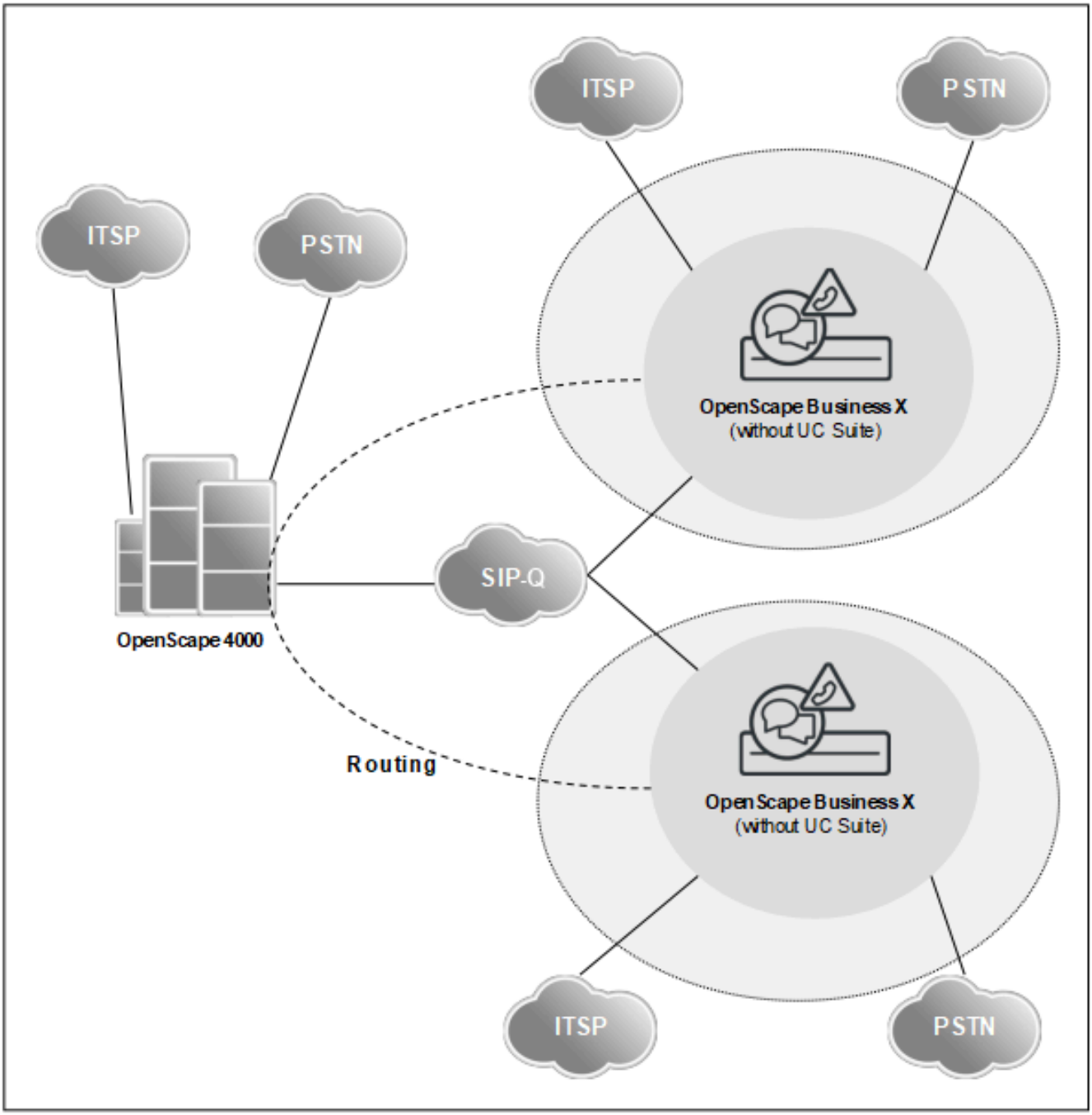
Scenario b: Internet work with OpenScape 4000 and Routing of all Connections via OpenScape 4000

Network Data



- Closed numbering within the OpenScape Business internetwork
- Network-wide voice and UC functionality within the OpenScape Business internetwork

- Configuring the OpenScape Business internetwork with the Networking wizard
- Configuring the OpenScape 4000 network components in Expert mode
- The Small Remote Site (SRS) concept is not supported
- UC functionality via the UC Booster Server or the UC Booster Card is optional.
- OpenScape Business S can be integrated in single or multi-gateway mode.



- Open numbering
- Network-wide voice functionality
- Every call to another node is routed via OpenScape 4000

- No UC solution in OpenScape Business because the internetwork uses open numbering
- The Small Remote Site (SRS) concept is not supported
- The configuration must be done in Expert mode for each node

Network-wide Features

Expansion	Closed numbering within the OpenScape Business internetwork (scenario 4a)	Open numbering (scenario 4b)
Maximum number of nodes	100 (32 released, depending on OpenScape 4000	
Maximum number of stations per system	Depending on the OpenScape Business X model	
Maximum number of stations in the network	1500 for the OpenScape Business network segment	Depending on OpenScape 4000
Voice networking	SIP-Q	

UC networking	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Network-wide functionality within OpenScape Business	Not supported
UC Booster Card	UC Smart: 51 - 150 stations (0 - 50 stations without UC Booster Card) UC Suite: 0 - 150 stations	Not supported
UC Booster Server	UC Smart: from 150 stations UC Suite: from 150 stations	Not supported
OpenScape Business S	Supported	Not supported

Administration	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	WBM with wizards for OpenScape Business nodes; OpenScape 4000 is administered via the Expert mode of OpenScape Business.	Network-wide administration in Expert mode
WBM	WBM with wizards	WBM with Expert mode
Manager E	Not recommended	Not recommended
UC Suite administration	WBM with wizards for OpenScape Business nodes	Not supported
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each node in the internetwork	

Licensing	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Licensing structure	A network license is required for each OpenScape Business	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Netwide with UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S	Not supported
Instant Messaging	Network-wide, within the OpenScape Business internetwork	Not supported
Voicemail	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Network-wide, within the OpenScape Business internetwork	Not supported
Busy indication	Network-wide, within the OpenScape Business internetwork	Not supported
Internal Directory / Favorites	Network-wide, within the OpenScape Business internetwork	Not supported
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	via LDAP	Not supported

myAttendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	With UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S	Not supported
Instant Messaging	Network-wide, within the OpenScape Business internetwork	Not supported
Voicemail	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Network-wide, within the OpenScape Business internetwork	Not supported
Busy indication	Network-wide, within the OpenScape Business internetwork	Not supported

myAttendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Internal Directory / Favorites	Network-wide, within the OpenScape Business internetwork	Not supported
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	via LDAP	Not supported

OpenScape Business Attendant	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	Interface limited to 8-digit phone numbers	Interface limited to 8-digit phone numbers
Presence Status	Network-wide	
Busy indication	Network-wide	
External directory	via LDAP	via LDAP
Central Attendant Console	Network-wide, within the OpenScape Business internetwork	

Company AutoAttendant (UC Suite)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Company AutoAttendant: after the AutoAttendant answers a call, the caller must dial the number of the station to which he or she wants to be connected.	CCV scripts allow you to dial station numbers from the internal directory within the internetwork.	Not supported
Personal AutoAttendant: after the Auto Attendant answers a call, the caller must dial a single digit to be connected to his or her call destination.	Any station number preconfigured by a UC subscriber is possible	Not supported

Company AutoAttendant (UC Smart)	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Company AutoAttendant (UC Smart)	Local	Local

myAgent	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
	With UC functionality via UC Booster Server, UC Booster Card or OpenScape Business S. All agents are registered on ONE node. Incoming CC calls via the local PSTN, ITSP and SIP-Q trunk circuits.	Not supported
Instant Messaging	Netwide	Not supported

myAgent	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Voicemail (Recording, Message Waiting Indication, Check)	Subscribers use their local voicemail system; there is no central voicemail for the entire internetwork.	Not supported
Presence Status	Netwide	Not supported
Busy indication	Netwide	Not supported
Agent status	Local	Not supported
Internal Directory	Netwide	Not supported
External directory	Local, via import of CSV files	Not supported
Search in external directories of other nodes	Not possible	Not supported
External Offline Directory (LDAP)	via LDAP	Not supported
Outlook Contacts	Local	Not supported
Transferring a Call	Local	Not supported
Customer information	Local	Not supported
Reporting	Local	Not supported

External applications	Closed Numbering (Scenario 4a)
OpenScape Business TAPI application	See Application Connectivity
External CSTA applications	
Application Launcher	
OpenScape Contact Center	See Multimedia Contact Center.

Telephony	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
SIP Provider (ITSP)	Local	Local
PSTN Provider	Local; network nodes without a PSTN provider of their own are reached via SIP-Q or the associated gateway.	
Survivability (redundancy in the event of an internetwork or OpenScape Business S breakdown)	Is supported between OpenScape Business X and OpenScape Business S	Not supported
Dial a public number in the own node	Supported	
Dial a public number in a networked node	Network-wide, within the OpenScape Business internetwork	

Mobility	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Desk Sharing	Within a node; network-wide, within the OpenScape Business internetwork (with DLS)	Not supported

Mobility	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Mobility with DTMF control of the system	Local (not supported for OpenScape Business S)	Local
myPortal to go (Web Edition), UC Suite	Network-wide presence status and directories (requires a UC Booster Server, UC Booster Card or OpenScape Business S for each node)	Not supported
myPortal to go (Web Edition), UC Smart	Local, not for UC Booster Server, UC Booster Card and OpenScape Business S	Not supported

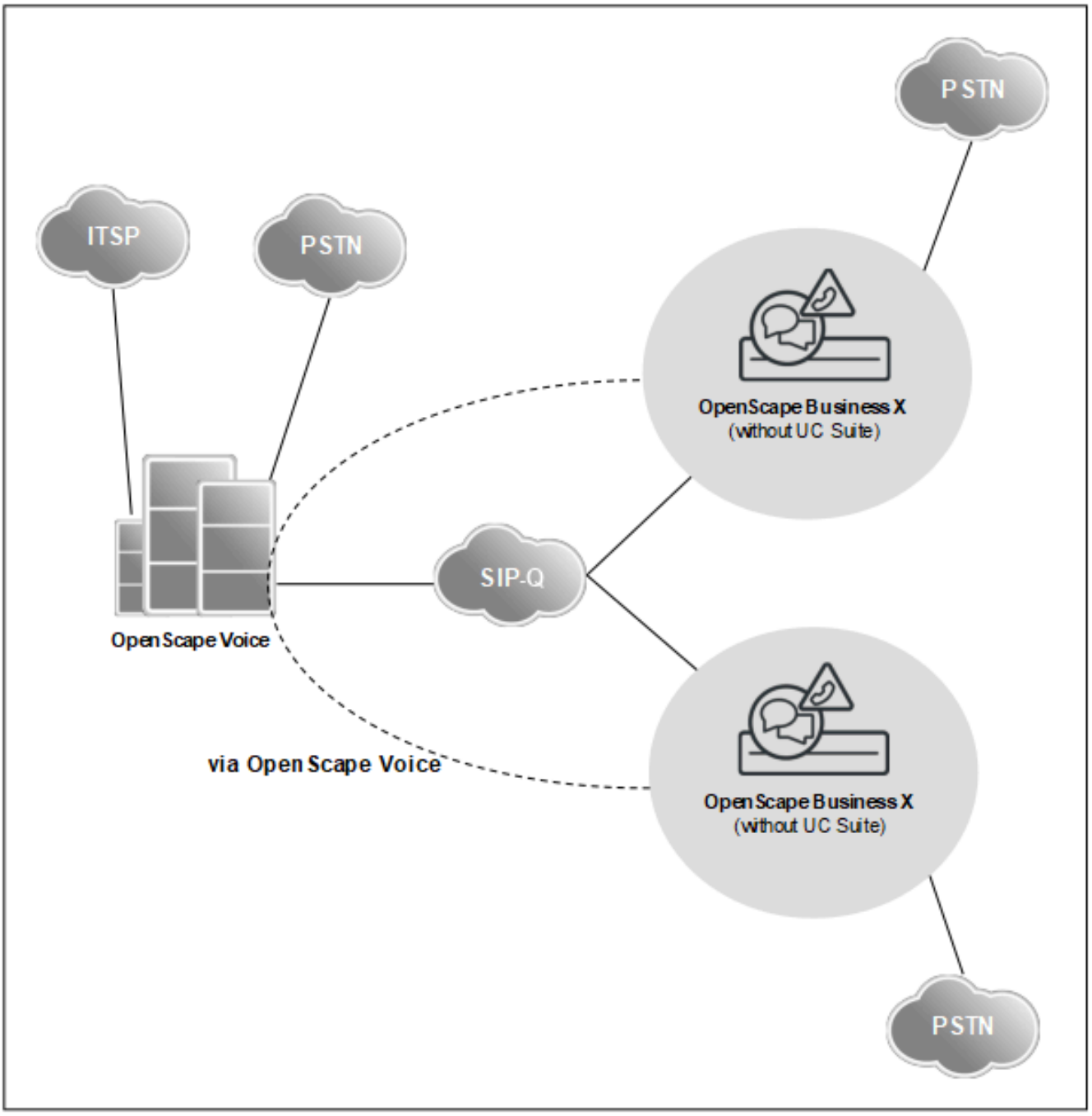
Other functionalities	Closed Numbering (Scenario 4a)	Open numbering (scenario 4b)
Signaling and Payload Encryption (SPE)	Not supported in OpenScape 4000 / OpenScape Business networks. Not supported for UC connections and conferences	Not supported in OpenScape 4000 / OpenScape Business networks. Not supported for conferences
DSS server	Network-wide, within the OpenScape Business internetwork	Not supported
Call Pickup	Not supported	Not supported

21.6.7 Networking OpenScape Business X and OpenScape Voice

OpenScape Business X can be networked with OpenScape Voice.

NOTICE: A configuration example for networking with OpenScape Voice can be found in the Unify Experts wiki at `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Network Data



- OpenScape Business X provides network-wide voice and gateway functionality for OpenScape Voice.
- One or more OpenScape Business X systems can be used as a gateway for digital Central Offices (ISDN, T1, CAS)
- The following devices can be operated at cape Business X gateways: digital / analog / DECT / IP (HFA)
- UC is generally not supported by OpenScape Business X in this networking scenario.
- Each call from one node to another is routed through OpenScape Voice.
- The configuration of each node occurs in Expert mode.

- The OpenScape Voice dial plan is based on E.164, which explains why neither open nor closed numbering is available.

Network-wide Features

Maximum configuration	
Maximum number of nodes	Depending on OpenScape Voice
Maximum number of stations in a single communication system	Depending on OpenScape Business X
Maximum number of stations in the network	Depending on OpenScape Voice

Administration	
WBM	The Networking wizard cannot be used. OpenScape Voice is administered per node via the OpenScape Business expert mode.
Manager E	Not recommended
UC Administration	UC is not relevant in connection with OpenScape Voice
Mass data import via CSV files (call numbers, DID numbers, names)	Separately for each of the nodes in the OpenScape Business internetwork

Licensing	
Licensing structure	Each node individually; a network license is required for each OpenScape Business node

Restrictions and Notes on the Features

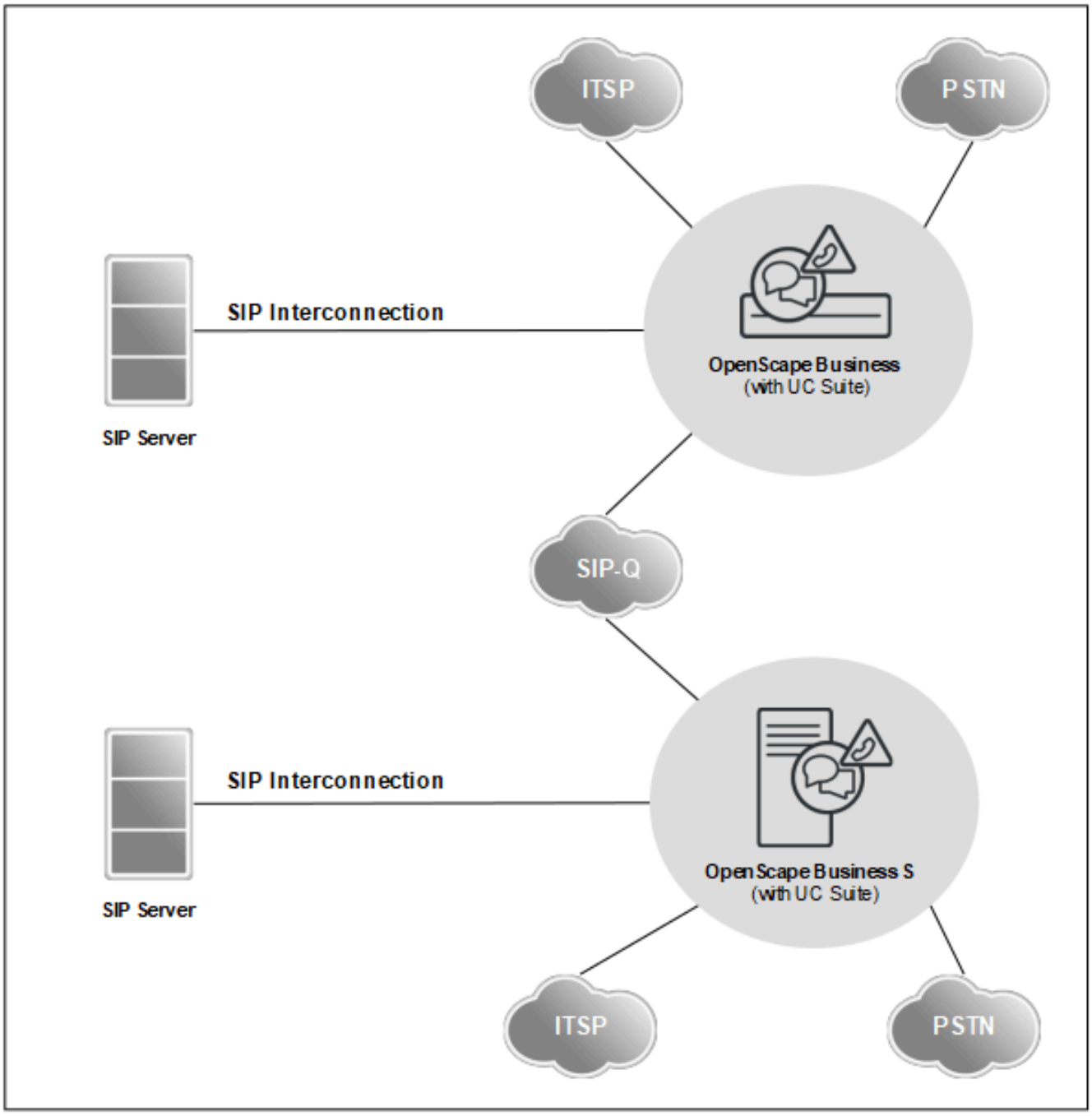
- The connection of analog CO trunks at OpenScape Business gateways is released **only** for Brazil (due to the support for line reversal and backward release of analog CO trunks in Brazilian COs).
- A network of OpenScape Business gateways with one another or with systems other than OpenScape Voice is not supported. The networking of the OpenScape Business gateways with OpenScape Voice must occur through a star-shaped network structure.
- Path replacement (route optimization) via SIP-Q is not supported for the devices connected to an OpenScape Business gateway.
- To avoid poor voice quality on transit line connections, the G.711 voice codec should be used. The G.729 codec is not recommended, since transit line connections can be caused by features such as conferencing and call forwarding. This is because path replacement (i.e., route optimization) is not supported.
- No cross-system support between OpenScape Voice and OpenScape Business gateways is available for features such as call pickup groups, group calls and hunt groups. The groups may include only subscribers of either OpenScape Voice or OpenScape Business, but not both.
- Encryption (SPE) between OpenScape Voice and OpenScape Business gateways is supported. The connection between OpenScape Voice and OpenScape Business must be made by means of the TLS encryption protocol. SRTP (SDES) is not supported in a network with OpenScape Voice V7R1.
- Networking is supported only with the E.164 numbering plan.

- The following applies to the IP stations (HFA) connected to OpenScape Business gateways: For each active OpenScape Business/OpenScape Voice connection, two B channels per HFA device are required (one B channel per TDM device). The need for these additional DSP resources should be reviewed and taken into consideration.

21.6.8 Connecting External Auxiliary Equipment to OpenScape Business via SIP Interconnection

External auxiliary equipment can be connected to OpenScape Business via SIP Interconnection, e.g., to use applications such as OpenScape Alarm Server, OpenScape 4000, OpenScape Voice or other certified SIP servers.

Prerequisites



- Only certified applications may be connected, for example, OScAR.
- An external SIP server can be connected via the Native SIP or SIP-Q protocol.
- A maximum of two SIP-Q routes (one is required for UC Suite, if present) and a maximum of 10 Native SIP routes (of which up to 8 Native SIP routes can be used for ITSP) are available.

Additional information can be found in the

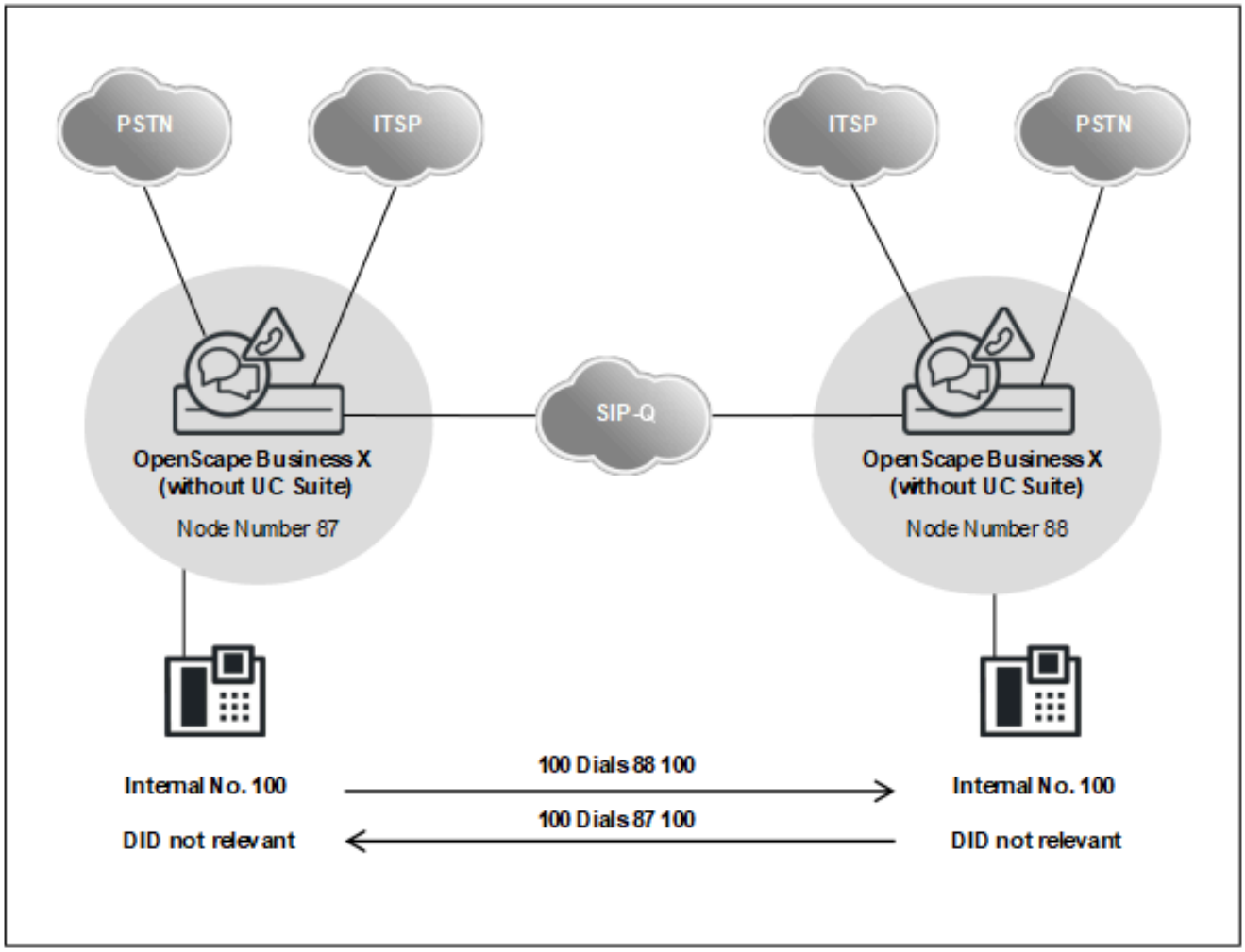
- Expert wiki for telephones, communication systems and UC:

  `http://wiki.unify.com`

21.6.9 Open Numbering in OpenScape Business X Networks

A internetwork with open numbering can be set up by networking two (or more) communication systems whose numbering schemes overlap one another (i.e., not unique throughout the internetwork).

Network Data



- Network-wide voice networking via OpenScape Business.
- UC features are not supported.
- Every call within a node occurs with an internal call number.
- Every call to another node occurs with a node number (plus an internal number).
- Each node must be configured in Expert mode. The Networking wizard is disabled once a node number for open numbering has been configured.
- Outside line access to the PSTN or ITSP is possible from each node.

NOTICE: In case of a network-wide extension on UC functionality, it is necessary to change from open to closed numbering in order to adapt the internal numbers. Thus, the open numbering must be disabled, while the node number must be deleted and subsequently added as a prefix (for example,

extended internal number 87100 instead of 100 and 88100 instead of 100).

Differences:

- The selection of participants in their own node is made with the extended internal number.

- The internal number and the DID number may differ if necessary, but the DID numbers must not be changed.

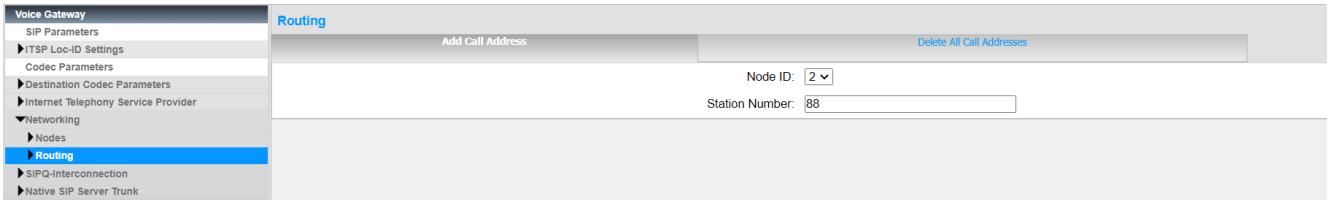
21.6.9.1 How to Configure Open Numbering

Configuring Open Numbering

1) Use the **Open numbering** system flag to enable open numbering for the communication system
2) Enter the number of your own node (e.g., "87")

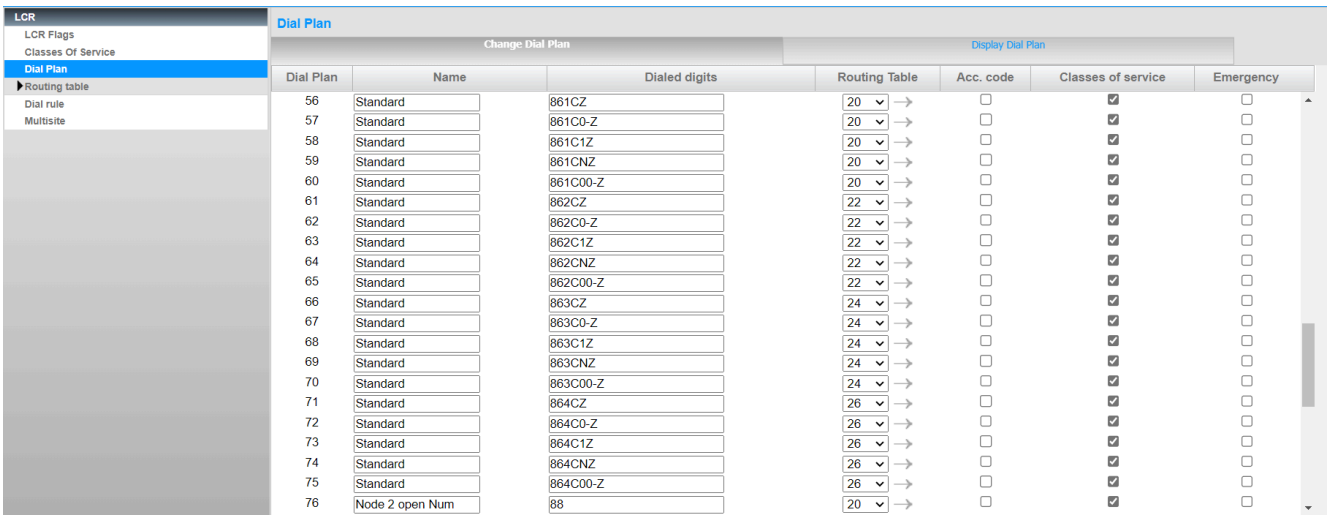
Configuring Nodes (Routing)

1) The destination nodes are addressed via Voice Gateway > Networking > Nodes > Routing (e.g., "88")
2) In an open numbering scheme, the **Networking** wizard cannot be used; this is prevented by the **Open numbering** system flag.

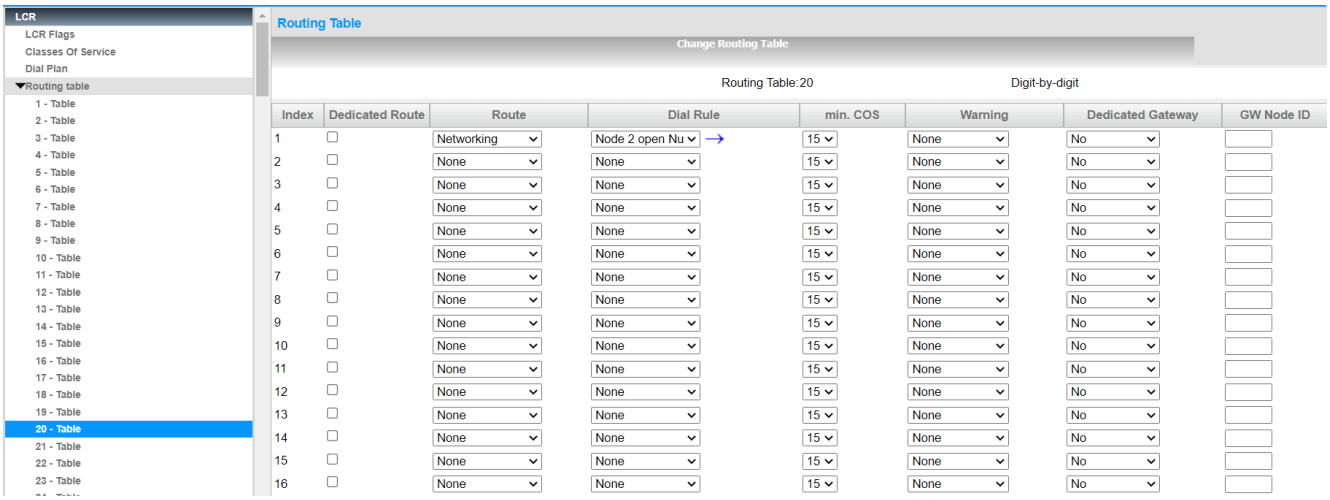


Configure LCR

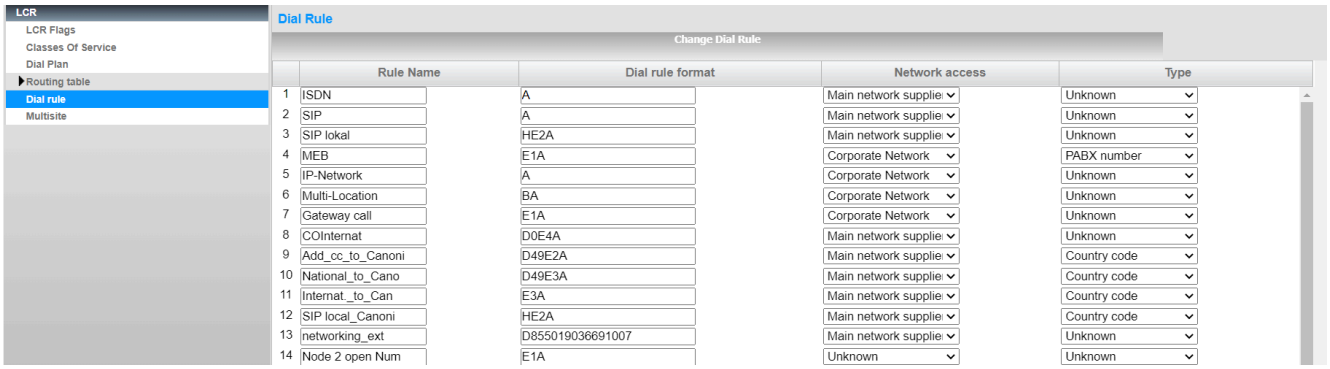
1) Assign the "Node 2 open Num" dial rule to the node number and select the associated routing table.



2) Display the configured route



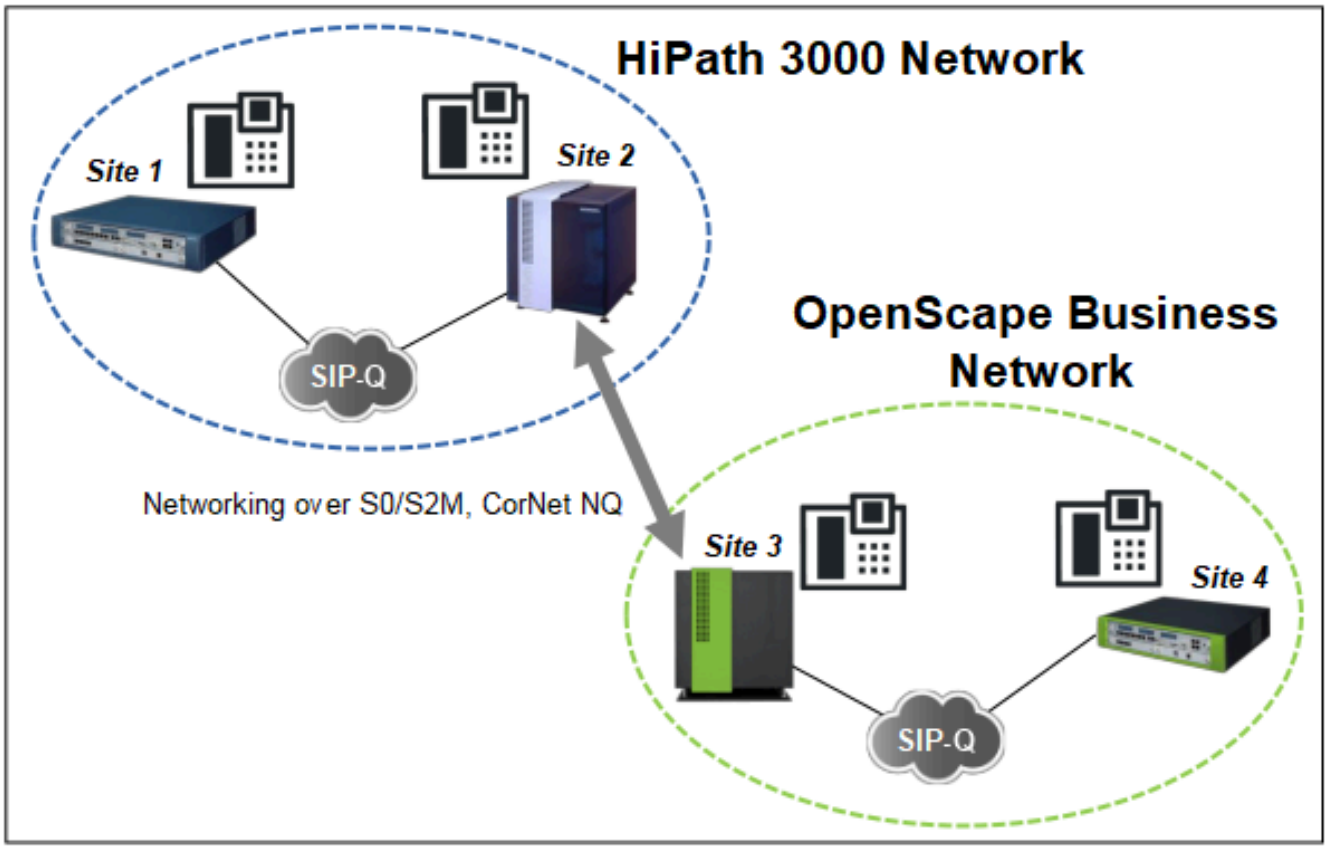
3) Enter the name of the "Networking" route and the dial rule "Node 2 open Num" associated with it.



21.6.10 Networking via ISDN

OpenScape Business systems can be networked with one another as well as with HiPath 3000 and OpenScape 4000 communication systems via digital trunks. Both S_0 as well as S_{2M} lines can be used for the connection.

Networking with HiPath 3000



The existing HiPath 3000 network is (initially) left intact. The expansion of the network occurs with OpenScape Business. HiPath 3000 nodes can be gradually migrated into the OpenScape Business network as required.

Every cross-network call that traverses the HiPath 3000/OpenScape Business is conducted via suitable TDM gateways (S_0 or S_{2M} with CorNet NQ protocol, possibly QSIG as a vendor-independent protocol).

The following constraints apply:

- Separate licensing for HiPath 3000 / OpenScape Business
- Separate administration for HiPath 3000 / OpenScape Business
- Recommendation: closed numbering in the overall network. Open numbering could potentially result in erratic behavior with CLIP and for journal entries / caller lists.
- Recommendation: use only the G.711 codec to ensure good voice quality in the overall network.
- The number of B-channels must be determined by taking the expected call volume into account.
- OpenScape Business requires a Networking license in any case.

Connection of External Systems via QSIG

The following must be noted when connecting external systems with the QSIG protocol:

- Check the QSIG variants of the external systems involved for compatibility (QSIG V1, also called QSIG as per the ECMA Standard, and QSIG V2, also called QSIG as per the ISO Standard)

- Compare the feature sets of the relevant systems. This should help to determine to what extent the theoretically expected scope of functionality, i.e., the intersection of both feature sets, corresponds to the customer's wishes.
- Furthermore, to guarantee the expected functionality, an on-site test of the connection is recommended. In particular, interworking with other networking and PBX protocols must be taken into account.

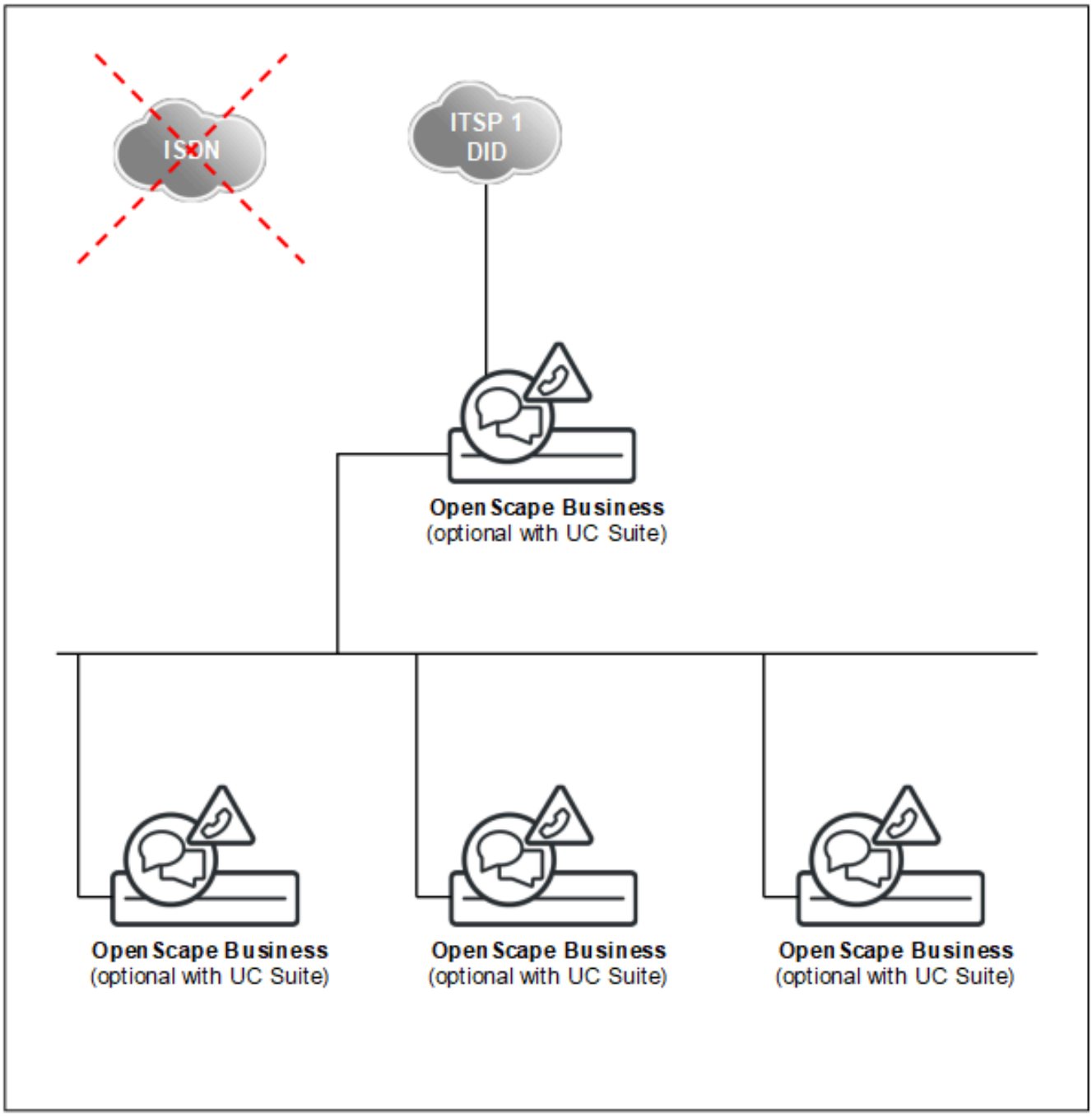
NOTICE:

QSIG trunk group should be configured as PABX route type in OpenScape Business system. Therefore, calls coming from QSIG network will be considered as internal and will follow internal CDL.

21.6.11 OpenScape Business internetwork with central ITSP trunk connection

A pure OpenScape Business internetwork can be implemented with a central DID-capable ITSP trunk connection instead of ISDN.

Networking with Central DID-capable ITSP Trunk connection



The following must be observed when planning customer networks:

- **One** central ITSP trunk connection for the entire OpenScape Business network.
- Registration at exactly one local network, i.e., all nodes in the network use exactly one Central Office number, e.g., 0049 89 7007-XXXXX.
- For emergency calls, the networked nodes can use their own trunk connections for outbound calls in cases where the central ITSP access fails. Under certain circumstances, a correct caller identification to the outside may not be possible in this case. Emergency calls, for example, may not be delivered correctly. Incoming accessibility via this local connection is

also subject to restrictions. For these reasons, local connections are not recommended, though not prevented technically.
- For the same reason, additional ISDN connections are not recommended (though technically not prevented) at the central node.
- All digit analysis and call routing rules for standalone OpenScape Business systems and networks apply. The station number assignment of the ITSP CO numbers occurs exclusively via the DID configuration of the station in this case (and not via the mapping table; see Configuring an ITSP in section 9.2 and the Unify Experts wiki on the Internet).

21.7 Central Intercept Position in the Internetwork (Not for U.S.)

OpenScape Business allows incoming calls that cannot be assigned to a station or answered to be diverted to a defined intercept position in the internetwork to ensure that no calls are lost.

If the central intercept position in the internetwork is configured using ISDN, then the functionality is identical to the functionality without networking.

In conjunction with an ITSP Central Office, the central intercept position is subject to some restrictions, since every node essentially has its own ITSP:

- The ITSP intercept criteria apply only to each respective node.
- The intercepts "on RNA", "on Device Busy", "on Incomplete", "on Invalid", and "on Unanswered Recall" work.
- The intercept types "on Invalid" and "on Incomplete" do not work with the ITSP.
- Incomplete or invalid telephone numbers are returned to the ITSP with a busy signal.

If a central intercept position is to be used in an internetwork, virtual stations must be configured in each node. These virtual stations are permanently diverted via the internetwork to the myAttendant user.

Example for an ITSP CO: ITSP PABX number is 0211-23456789 + ITSP DID number; the number 0211-23456789-0 is publicly announced as the central number of the communication system.

- Station 100 is myAttendant with its own ITSP DID number 100 and a virtual station 199 with the ITSP DID number "0".
- In the ITSP mapping list of each node, the ITSP DID number "0" is assigned to the own virtual station.
- Under **Incoming Calls/Call Forwarding**, the virtual stations are referred to station 100.

  First destination: own virtual station

  Second destination: station 100 in the destination node

  Call time 5 seconds

For better identification of calls, it is recommended that the virtual stations of all nodes be provided with their call number (DID) and a name (e.g., company) via the myAttendant application (under **Setup**/**myAttendant**/**DIDs**). This enables a more detailed identification of the caller in the **Active Calls** window of myAttendant.

21.7.1 How to Configure a Central Intercept Position in the Multi-Gateway Internetwork

This configuration example shows you how to set up a central intercept position in the multi-gateway internetwork via the upstream OpenScape Business gateways. All calls which are received at a node and which meet the intercept criteria must be routed to OpenScape Business S, where the central AutoAttendant is located.

Prerequisites

OpenScape Business S is the master (all HFA and SIP stations are logged in here).

Multiple OpenScape BusinessX systems have been set up as slave nodes (with PSTN or ITSP as the outside line). The nodes may be at the same location or at different locations (with different prefixes).

Step by Step

1) Set up a virtual station at the OpenScape Business.

a) Set up a virtual station with the name "Intercept 22 System2"

2) Set up a central intercept position with intercept criteria at the OpenScape Business.

a) **Expert mode**

b) **Basic Setup** > **System** > **Intercept/Attendant/Hotline**

c) Select virtual station 22 under **Intercept position** for **Day and night**.

d) Enter the following parameters for station 22 under **Intercept position** for **Intercept**:

Name	Intercept 22 System2
Direct inward dialing	xxxxxxx22
Device type	Virtual

e) Activate the entered parameters under **Intercept position** for **Intercept**.

f) Set up the virtual station under **Intercept position** for **Lock Code**.

3) Set up the call forwarding OpenScape Business.

a) Set up the call forwarding of the virtual station 22 via the internetwork to OpenScape Business S.

b) **Expert mode**

c) **Incoming Calls** > **Call Forwarding**

d) Select virtual station 22

e) Proceed with **Edit Call Forwarding**

f) Then go to: **External destination** (enter the station numbers for the AutoAttendant queues, e.g., 7410)

g) **Route** = Select network (the AutoAttendant queue station number 7410 must be specifically routed in the LCR by bypassing the -Z default rule 33).

4) Configure the routes for OpenScape Business.

The AutoAttendant queue station number 7410 must be specifically routed in the LCR by bypassing the -Z default rule 33.

Under **Dial Plan**:	Configure the **Name** (VSL Queue Pilot)

	Enter the station number (7410) under **Dialed digits**
	Select **Routing Table** (XX)
Under **Routing Table** XX:	Select **Route** = Network
	Assign Dial Rule
	Under **Dedicated Gateway**, select the entry **Mandatory**
	Enter the **GW Node ID** of the OpenScape Business S.
Under **Dial Rule**:	Enter the **Rule Name**
	Under **Dial rule format**, enter D7410 (Queue Pilot Number)
	Under **Network provider's method of access**, select Corporate Network
	Type: Select Unknown

5) Set up a queue at OpenScape Business S.
   a) Set up a queue (Queue Pilot) with a CCV, e.g., **Dial By Extension**, **Dial By Name**, **Process after digits**.

6) Set up call forwarding at OpenScape Business S.
   a) Set up call forwarding of the Queue Pilot 7410 in OpenScape Business S.
   b) **Expert mode**
   c) **Incoming Calls** > **Call Forwarding**
   d) Select Queue Pilot 7410
   e) Proceed with **Edit Call Forwarding**
   f) First go to: **External destination** (enter the station numbers for the AutoAttendant queues, e.g., 7410)
   g) Then go to: select the **Voicemail box**

21.8 Presence Manager

Presence Manager enables the subscriber states "Free", "Busy" and "Ring" to be signaled throughout the network at the LEDs of the HFA telephones. This requires closed numbering and at least one UC Booster Server at the master node of the internetwork or an OpenScape Business S as the master node. A network license is required for each node.

In the idle state, the corresponding LED is off; in the busy state, it is constantly on, and in the ringing state, the LED flashes. In the ringing state, the call involved can be picked by pressing the corresponding button.

Call processing states can only be signaled for a station if the Presence Manager can set a CSTA monitor point on the relevant station.

The keys are configured by the user. When station numbers are programmed on the telephone itself, no distinction is drawn between internal and network-wide numbers.

The Presence Manager is a service and has no user interface. No settings need be made, as all data is automatically obtained through data synchronization.

Groups are not supported by Presence Manager. LED signaling is not performed and call pickup is not possible. MULAPs, however, are not supported by Presence Manager.

Presence Manager does not actively support any SIP and S_0 phones.

21.9 Synchronization Status in the Internetwork

In an internetwork, the synchronization status is displayed in the Admin Portal, and the registration status of each node is indicated by colored buttons.
The display of the synchronization status applies to network nodes of the communication system, but not to OpenScape 4000 and OpenScape Voice nodes.

Display of the Synchronization Status

Display	Color	Meaning for the master	Meaning for the slave
Synchronization status (display on the home page of the Admin Portal)	Red	-	The IP address of the master node is configured, but the slave system could not register. The slave tries to register with the master at cyclical intervals.
	Yellow	-	The slave is registered with the master, but the call numbers are not consistent in the internetwork. This may occur after a backup/restore or after the first registration.
	Green	If a node is configured as the master, the status appears as green.	
Registration status of the individual nodes (displayed in the Network>Node View dialog)	Red	The slave is configured, but the system has never registered.	The slave is configured, but the system has never registered.
	Green	The system is registered.	The system is registered.
Alive (displayed in the dialog Network>Node View)	Red	Node-specific view of the internetwork: all nodes that are marked in red cannot be reached. The reasons may be network problems or a failure in the communication system.	
	Green	The (external) node can be reached via the network. The own node is always shown in green.	

21.9.1 Manual Synchronization in the Internetwork

If the automatic synchronization of the configured call numbers and names (internal or DID numbers) has not been completed in the other systems of an internetwork, a manual synchronization can be initiated. This manual synchronization in the internetwork only works in homogeneous networks.

Master

Slave

The synchronization process only transfers changes in the configuration.

If the status indicator in the Admin Portal appears as "red", the Synchronization button can be pressed to try and manually synchronize the data with the master.

In cases where already configured systems in the network can no longer make calls, the potential cause for the problem must be found elsewhere. If the Alive status of individual nodes appears as "red", this indicates network problems or other reasons why the node cannot be reached in the network. In such cases, activating the Synchronization button will not improve the situation.

When activated on the master node, the slave nodes are requested to update the phone numbers and names of the system from the master.

When activated on a slave node, the station numbers and names of the system are updated on the master. At the same time, the slave node is registered again at the master node.

21.9.2 How to Start Synchronization Manually

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

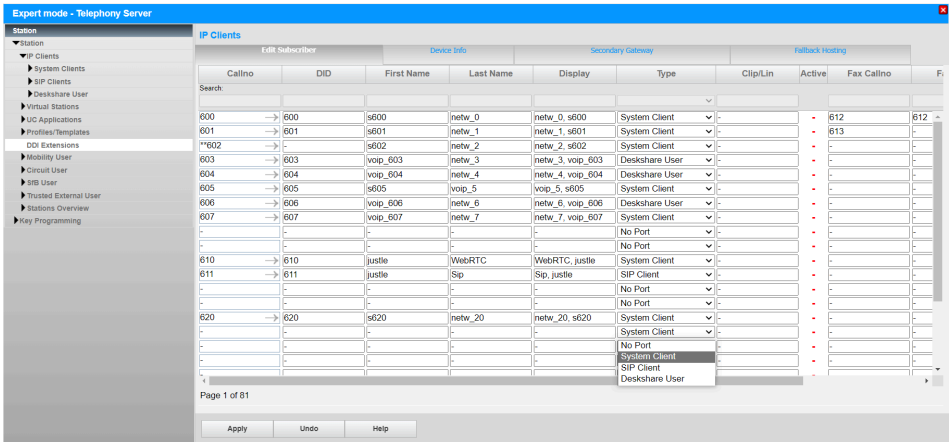
Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Activate the **Sync Network** button to start the manual synchronization.

21.10 Survivability

Survivability is a feature within a network of OpenScape Business nodes. If an OpenScape Business node fails or cannot be reached due to network errors, the system telephones (HFA) logged in at the OpenScape Business node can log in at the other OpenScape Business node of the network instead. The phone numbers of the system telephones are retained after the new login. This provides continuity for basic telephony; however, the features of applications

such as myPortal, voicemail and CTI will be temporarily unavailable.



When the OpenScape Business node that failed can be securely accessed again, the system telephones automatically revert to the OpenScape Business node.

The time for switching to the standby gateway can last up to 30 minutes.

If the OpenScape Business node fails, an attempt is first made to reach it again for a fixed time period (10 minutes; cannot be changed). It is only when this time has expired that the system telephones intended for this purpose are registered at the standby gateway. The current statuses of the registered phones can be viewed in **Expert Mode** > **Diagnosis Logs**.

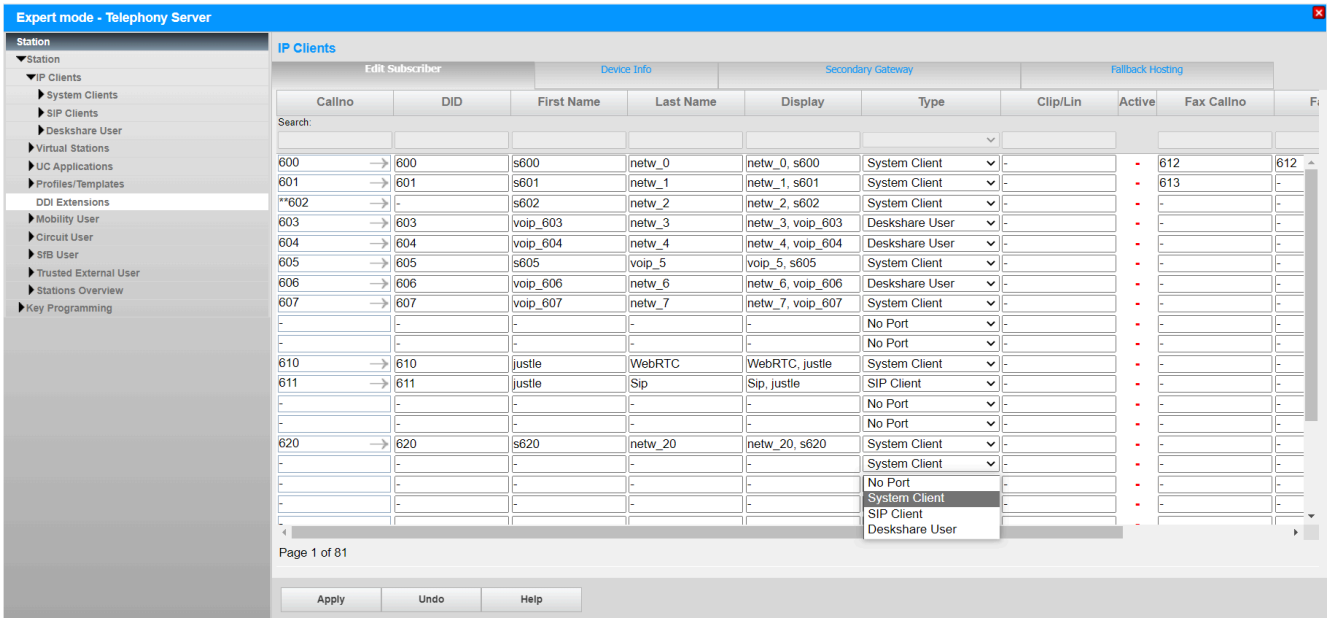
The survivability settings are configured at the system telephones. If the OpenScape Business node fails, the phones will initially try to reach it again several times. A time-out or how often the phone tries to log in again can be configured via the "System Redundancy" setting on the Administration menu of the telephones. The default setting for the timeout is 30 seconds with one retry. After that, the telephones register at the standby gateway. The automatic registration back at the OpenScape Business node must also be configured at the system telephones.

NOTICE: The survivability feature requires the POSTGRES service to function correctly. If the Application Firewall is enabled with a rule for the POSTGRES service then you must ensure that the IP addresses of the other networked OpenScape Business nodes are manually added to this rule otherwise the survivability feature will not function.

The following prerequisites must be satisfied for survivability:

- A sufficient number of free IP ports must be available at the standby gateway for the system phones connected to the OpenScape Business node that need to be "saved" when a network node fails.

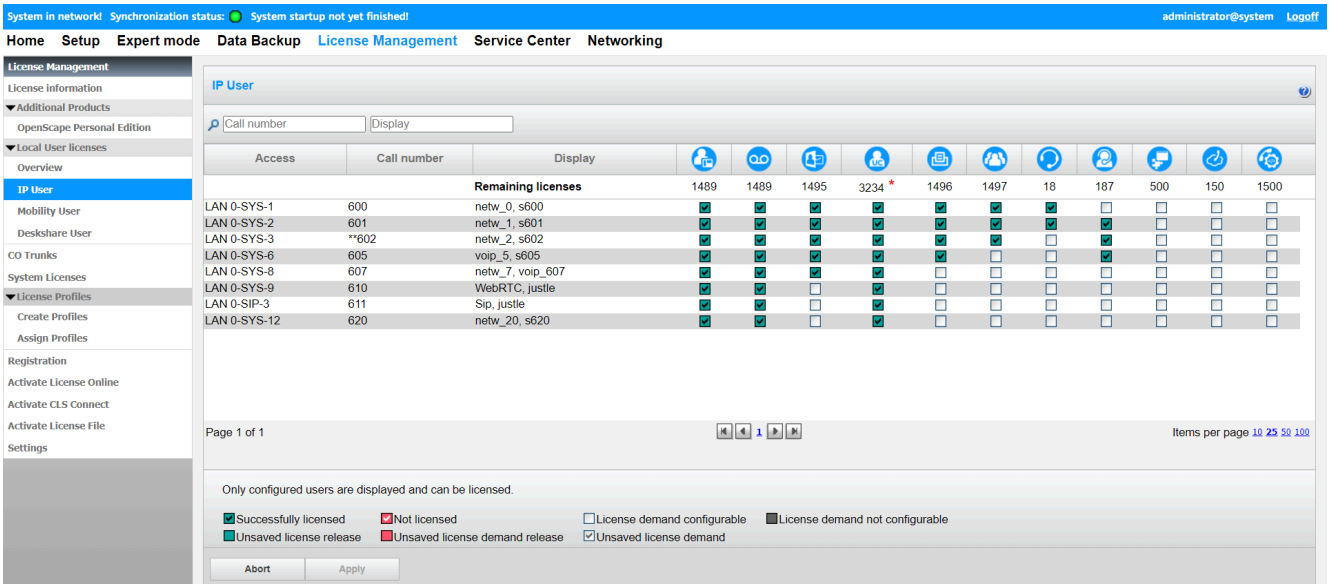
- For these free ports on the standby gateway, stations must be set up without a name and phone number.



- The stations must be configured as system phones (system clients) and have a Fallback user license. If Fallback licenses are not available in the activated license file, IP user licenses can be used instead. In the event of survivability, the stations can only use telephony features.

NOTICE: During the downtime of the master node HFA redundancy clients call numbers conflict until the master node is up and running again.

NOTICE: If the system has Fallback user licenses assigned, then IP user licenses cannot be used in case of an event of failure.



21.10.1 How to Configure Survivability

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Navigate in the menu tree to **Stations** > **IP Clients**. In the case of an OpenScape Business master system, the **Secondary Gateway** window appears.
3) Under **Node ID**, select the OpenScape Business to which OpenScape Business S users are to be transferred in the event of an emergency.
4) Select the **Emergency** check box for the emergency station.
5) The entries for **Emergency Call no** and **Call no DID** are preset and can be adapted if required.
6) Click on **Apply** followed by **OK**.

21.11 Removing a Node from the Internetwork

If a node is to be removed from the internetwork, it must first be ensured that the node is no longer available in the network configuration. Otherwise, the node will independently attempt to register itself again in the network and master node will try to synchronize data.

Procedure

The deletion of a node occurs via the Networking wizard, where all nodes involved must always be removed.

- Interrupt all paths (routing) to the nodes to be removed
- Administration of the internetwork
- Enter "No network" for the slave node involved in the networking wizard of the slave node.
- Remove the slave node from the registration list in the networking wizard of the master node.

If o node is not removed properly, data will continue to be transferred from one OpenScape Business to another and thus produce inconsistencies in the internal directory, i.e., the users will not appear in the user directory and will therefore be unable to use myPortal for Desktop.

22 Auxiliary Equipment

Auxiliary equipment consists of external devices (such as an announcement device or an entrance telephone with door opener) that are connected to the interfaces of the communication system.

22.1 Analog Announcement Device

An analog announcement device can be connected to an a/b interface to play custom announcements (e.g., for the central AutoAttendant or as a replacement for music on hold).

NOTICE: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

Up to 16 announcement sources (e.g., media servers, announcement players or analog announcement devices) can be configured for each communication system.

The following types of announcement devices can be used:

- Announcement devices that always start at the beginning of the message when activated (such as greeting messages).
- Continuous playback devices (e.g., for music on hold)

The announcement device must behave like a station, i.e., announce itself, play the announcement and switch the call (enter consultation hold, dial and hang up).

Announcements Types

The following types of announcement are available:

- Greeting announcement (announcement prior to answer)

  A greeting announcement can be played to callers prior to answering their calls.
- AutoAttendant

  When the AutoAttendant is enabled, music and/or further announcements can be played to callers if they cannot be switched immediately.
- DTMF DID

  When DTMF direct inward dialing is enabled, an announcement lets callers know that they can use DID to dial another extension. During the announcement, a code receiver detects if the caller uses suffix dialing and then forwards the call to the number dialed.

Alternatives to the A/B Interface (SLA Boards)

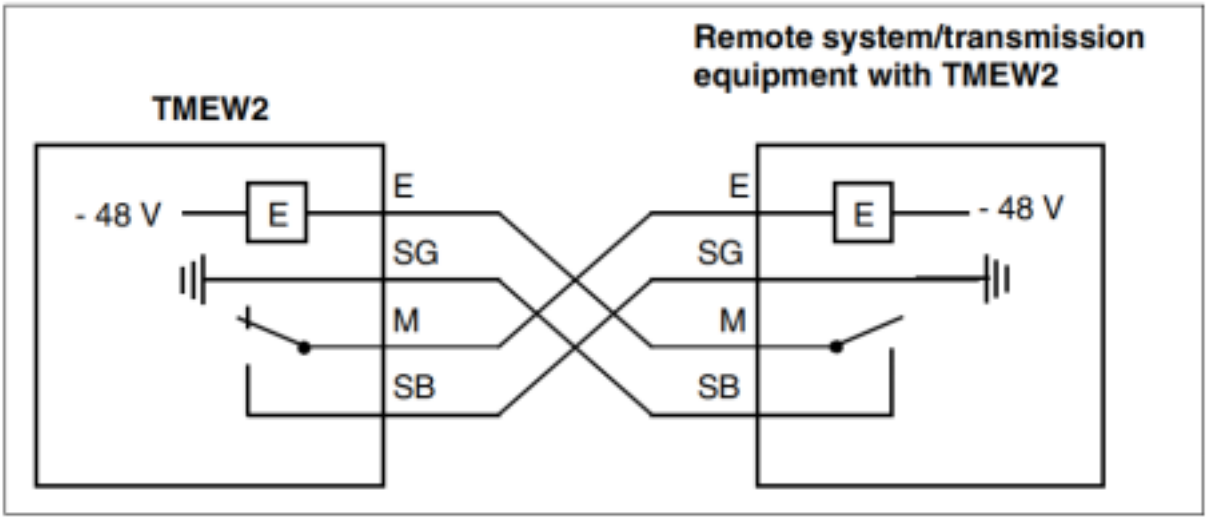
- OpenScape Business X8: TMEW2 board
- OpenScape Business X5: Optional STRB Board
- OpenScape Business X3: Optional STRBR Board

Announcement Delay Time

The announcement delay time is the time (0 - 600 s, configurable) which must elapse before a waiting call is forwarded to an announcement device.

Announcement Device - Genius

The TMEW2 board may be installed on interface type 2 for connecting the Genius announcement device. A description of the TMEW2 board and the assignment of SIVAPAC connectors on the backplane when connecting the Genius announcement device can be found in the Service Documentation, Hardware Installation, Chapter "Boards".



The configuration of the Genius announcement device is performed in Manager E via **System View** > **Settings** > **Auxiliary Equipment** > **Announcement**.

22.1.1 How to Add an Analog Announcement Device

Prerequisites

Your announcement device is connected to an analog interface.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Telephones / Stations**.
3) Click on **Edit** to start the **Analog Terminals** wizard. A list of all analog stations appears.
4) Enter the names and phone numbers in the row of the announcement device.
5) If necessary, make additional settings in the row of the announcement device.
6) Click on **OK & Next** followed by **Finish**.

22.1.2 How to Change the Announcement Delay Time

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

In the **System View** under the **Settings** > **System Parameters** > **Time Parameters** menu: In the **Delay for announcement prior to answer** entry in the table, set the **Base** and **Multiplication factor** of the announcement delay to suit your needs (default: 100ms x 20).

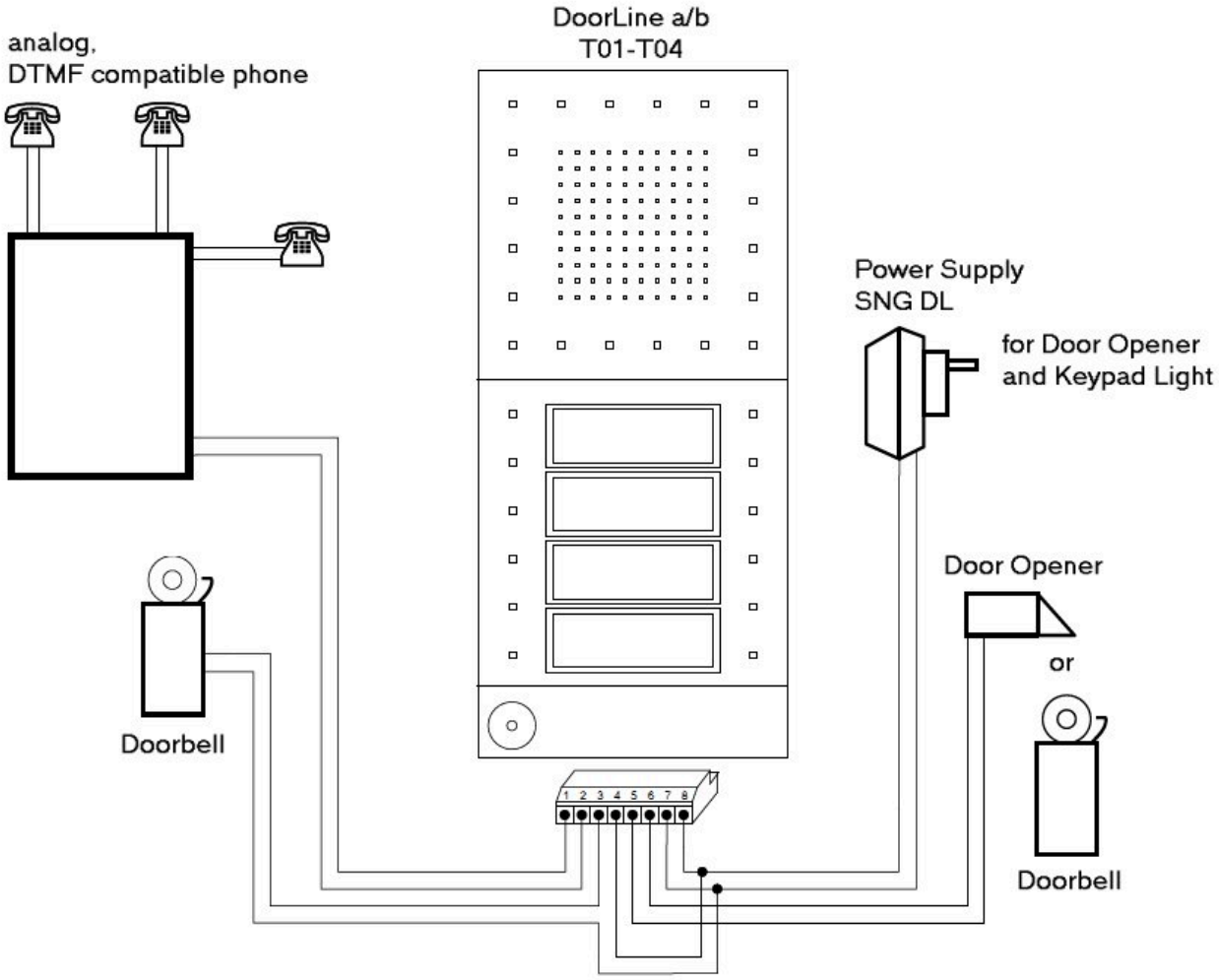
22.2 Entrance Telephone and Door Opener

Entrance telephones (ET) are offered in a wide range of options from several different manufacturers today. The available connection options are essential for the operation and functionality of each ET. The Doorline a/b T01-T04, which is similar to other door openers by Behnke, Keil, 2n EntryCom, Auerswald, etc., is described here as an example.

22.2.1 DoorLine a/b T01-T04

The door opener DoorLine a/b T01-T04 is connected to an analog port. Equipped with 1 to 4 bell buttons (depending on model), several independent residential and commercial areas can be reached. The DoorLine a/b T01-T04 can not only be operated from any phone, but also provides the connection for the power supply of the door opener.

Due to the 2-wire a/b technology, the DoorLine a/b T01-T04 can be quickly and easily mounted. To synchronize with the communication system, the dialing method can be set, and the voice channel can be matched. The door is opened via the code of the Doorline (e.g., #9). A special interface module such as the Doorline M02, M03, M06 and M06/1 is no longer necessary.



NOTICE: No further setting is required in OpenScape Business for this entrance telephone/door opener. For security reasons, it is recommended that the extension be configured with "no trunk access" or with "outward-restricted" trunk access.

22.2.1.1 How to Configure the Station Port of the DoorLine a/b T01-T04

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

1) Under **System view**, in the **Settings** > **Set up station** > **Stations** menu, select the type **Standard** for the station port.
2) Under **Station view**, on the **Flags** tab, enable the flag **Call waiting rejection on** for the station port.
3) Under **System view**, in the **Settings** > **System Parameters** menu, on the **Flags** tab, enable the flag **DTMF automatic** .

22.2.1.2 How To Configure the Extension for the Doorline a/b T01-T04

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

1) Under **Station view**, on the **Flags** tab, enable the flag **Call waiting rejection on** for the extension.
2) Under **Station view**, on the **Flags** tab, enable the flag **Missed Calls List** for the extension.

22.2.2 DoorCom Analog

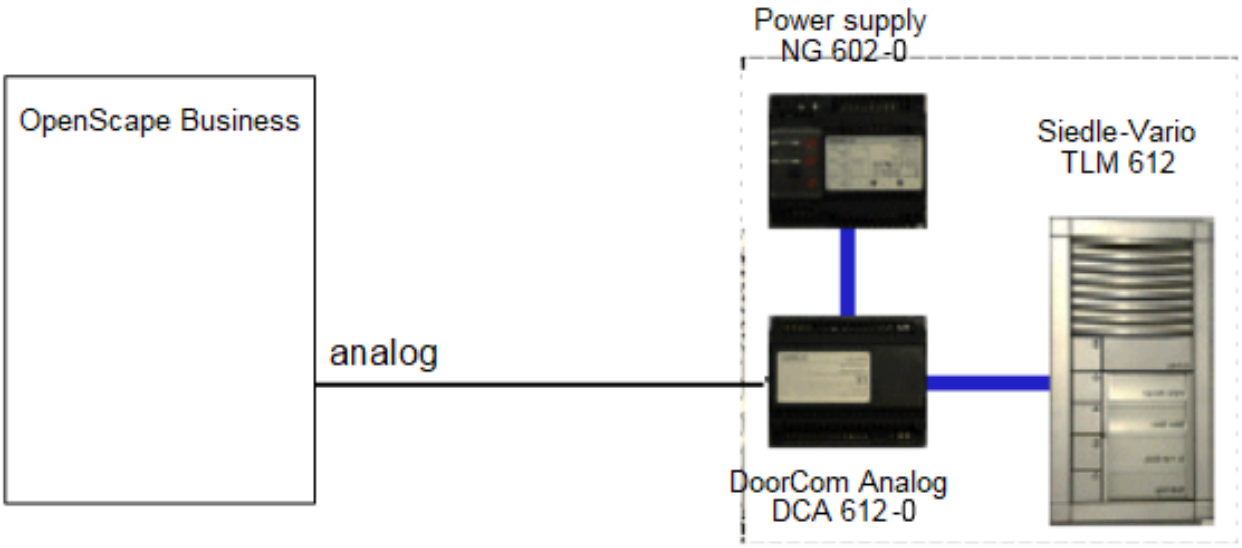
DoorCom® Analog is a universal entrance telephone adapter box for Siedle entrance telephones (such as the Vario TLM 612).

The DoorCom® Analog is connected to an analog port of the communication system. It behaves like an analog telephone with DTMF dialing, DTMF detection and DTMF control. It can be operated with DTMF signals.

DoorCom Analog can function only in combination with the following components:

- DoorCom Analog DCA 612-0
- Siedle-Vario TLM 612 entrance telephone
- Switching remote control interface DCSF 600

  For the voice connection of an internal user to the entrance telephone. Without this module, it is not possible to call back to the entrance telephone, for example, if a call was unintentionally cleared down by the entrance telephone.
- Power supply NG 602-0



Device control features (open doors, select entrance telephone, etc.) can be programmed on the procedure keys of a phone. The programmed DTMF signal sequence is then sent to the entrance telephone/door opener.

NOTICE: No further setting is required in OpenScape Business for this entrance telephone/door opener. For security reasons, it is recommended that the extension be configured with "no trunk access" or with "outward-restricted" trunk access.

22.2.2.1 How to Configure the Station Port of the DoorCom Analog

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

1) Under **System view**, in the **Settings** > **Set up station** > **Stations** menu, select the type **Standard** for the station port.
2) Under **Station view**, on the **Flags** tab, enable the flag **Call waiting rejection on** for the station port.
3) Under **System view**, in the **Settings** > **System Parameters** menu, on the **Flags** tab, enable the flag **DTMF automatic** .

22.2.2.2 How to Configure DoorCom Analog Extensions

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

1) Under **Station view**, on the **Flags** tab, enable the flag **Call waiting rejection on** for the extension.
2) Under **Station view**, on the **Flags** tab, enable the flag **Missed Calls List** for the extension.

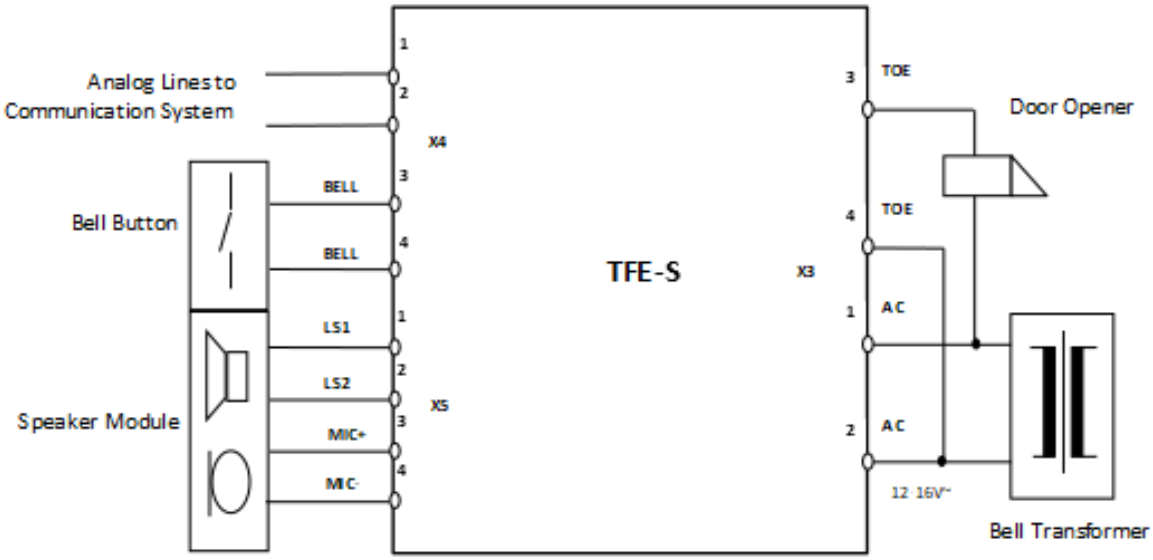
22.2.3 Entrance Telephone with Amplifier (TFE-S)

The TFE-S module (S30122-K7696-T313) connects an analog interface of the communication system with an entrance telephone, a door opener and a doorbell button. Control occurs via the communication system.

This makes it possible to connect to passive entrance telephones, which are comparable with the following types:

- From the company Siedle (TLM511-01, 611-01)
- From the company Rito (5760)
- From the company Grothe (TS6216)

The amplification can be adjusted manually. The TFE-S module requires its own power supply.



Technical Data

Parameters	Value
Power supply	Bell transformer 12V - 16V AC, 50Hz
Current draw	Max. 150 mA
OpenScape Business interface	Analog station
Dimensions	100mm x 160mm (5.7" x 9.1")
Ambient temperature	0°C to + 45°C

Functional description

Doorbell activation is signaled as a call at the phone of any configured station (ring destination). A voice connection to the entrance telephone is set up when the subscriber accepts the call. Additionally, the subscriber can also activate the door opener on his or her phone.

The call is intercepted if the entrance telephone ring destination is not reachable. If the intercept destination is busy, a system search is performed across all system phones.

INFO: The night service is ignored when signaling a door call.

INFO: System speed dialing at the entrance telephone is not possible.

Configuration Options

The following configuration options are available:

- Door opener:

  The door opener is configured via an a/b (T/R) interface and the entrance telephone must be connected via an adapter. The subscriber can then open the door by simply pressing a button on the phone during the connection with the ring destination.
- DTMF:

  This setting specifies whether the door opener is activated by a DTMF transmitter (DTMF: dual-tone multifrequency), that is, if the ring destination can open the door with DTMF suffix-dialing.
- Call Forwarding (CF):

  This specifies whether the call from the entrance telephone should be forwarded to an external call forwarding destination.

22.2.3.1 How to Configure the Entrance Telephone

The **Door Opener** wizard can be used to specify which subscribers are allowed to operate the door opener. You can configure up to ten entrance phones.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Door Opener** wizard. The **Edit Door Opener** window appears.
4) Select one or more **Stations**.
5) Enter the **Destination**.
6) Select the relevant functions such as **Door Opener**, **DTMF** and **FWD** in the check box.
7) Click on **OK & Next** followed by **Finish**.
8) Follow steps 1 to7 to configure each entrance phone.

22.2.4 Loudspeakers

Speakers can be connected to the communication system via an amplifier.

The following options are available for connecting an amplifier, including the loudspeaker:

- **Connection of the amplifier at an analog station interface**

  A level adjustment of the amplifier may be required for this.



- **Connection of the amplifier to the entrance telephone module TFE-S**

  An active amplifier / sound system can be connected via the TFE-S module. The amplifier input is connected to the speaker output of the TFE-S module.

  Furthermore, a contact of the STRB board may still be required to turn on the amplifier or switch through the input signal (noise suppression).

22.2.4.1 How to Configure the Analog Station Interface for a Loudspeaker

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Telephony** > **Stations**.
3) In the menu tree, click on **Stations** > **Analog Stations**.
4) Select the desired analog station (e.g., 3011).
5) Edit the data of the analog station as needed on the **Edit station parameters** tab.
6) Select the item **Loudspeaker** in the **Extension Type** drop-down list.
7) Click on **Apply**.

22.2.4.2 How to Configure the Analog Station Interface for Connecting an Amplifier to the TFE-S Module

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Door Opener** wizard. The **Edit Door Opener** window appears.
4) Select a **Station**.

5) Select the **Destination**.
6) Click on **OK & Next** followed by **Finish**.

22.3 Relays

Actuators are control outputs which are activated or deactivated by control signals from the communication system. They cause a change in the state of the connected equipment and support functions for monitoring, alerting, control and regulation. They are mainly used in security and building management systems (e.g., for door openers).

Actuators are contained in optional control relay modules. All control relay modules include four control outputs (actuators).

Possible control relay modules:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

The detailed description of these boards, including the assignments, can be found in the Service Documentation in the section on "Boards".

Actuators can be controlled in one of the following ways:

- from the phone by entering codes
- from the system phone by pressing a key
- remotely via a CO trunk (DISA) by the station assigned to the relay function
- remotely via the "Associated Services" feature

Actuators can be enabled or disabled using the following functions:

NOTICE: The control codes can be found the "Expert Mode" section.

- **No function**

  The actuator is either not operational or entered as a common ringer/night bell (under "Settings" - "Incoming calls" - "Call destination lists").
- **Manual on/off**

  The actuator can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations.
- **Auto off on timeout**

  The actuator acts as a time switch and can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations. If a value greater than 0 is entered for the switching time, the actuator is deactivated only when the switching time has elapsed.
- **Door opener**

  The actuator acts as a door opener and can be activated or deactivated via a key or via the "Activate/deactivate selected switch" code. This function can be assigned to a station, a group or all stations. If a value greater than 0 is entered for the switching time, the actuator is deactivated only when the switching time has elapsed. The text "Door opener" appears on the display

of all associated telephones. Example for the switching time multiplication factor: 30*100ms = 3 sec

- **Speaker amplifier**

  The actuator is activated when a connection is set up to the entrance telephone/door opener/loudspeaker. It is deactivated as soon as the connection is interrupted. This makes it possible to control an entrance telephone amplifier so that it is only activated when required. An entrance telephone or the loudspeaker port must be allocated to this function.

- **Busy indication**

  The actuator is activated when the associated station leaves the idle state (i.e., goes off-hook or activates the loudspeaker or receives an incoming call). The actuator is deactivated once the associated station re-enters the idle state. The actuator can also be directly activated via a key or via the "Activate/deactivate selected switch" code. In this case, the status of the associated station is ignored and the actuator can only be deactivated via a key or a code. A specific station must be allocated to this function. Example - Door busy indicator: If the Executive is on the phone, the door busy indicator lights up to show that he or she does not want to be disturbed.

- **Music On Hold**

  The actuator is activated if at least one station or a line in the communication system is not in the idle state. In this case, an announcement device or a CD player is activated. The actuator is deactivated if all stations and lines in the communication system are in the idle state. This function can only be assigned to all stations and must only be used once in the communication system. The value for the switching time must be greater than 0 (for example, 600*100ms = 60 sec). The actuator remains active and plays music until the switching time has elapsed or until it is disabled by a control signal.

- **Secondary bell**

  The actuator is activated for the allocated station if that station is being called. The actuator is deactivated when the called party answers or the call is terminated. The actuator is not clocked. A specific station must be allocated to this function. If a value greater than 0 is entered for the switching time, shutdown can be delayed. The switching time is a multiple of 3 seconds.

- **Call charge pulse**

  The actuator is clocked in accordance with the number for the allocated station on the basis of the incoming call charge pulses or call charge signals. A specific station must be allocated to this function. The switching time is 150 ms pulse and 150 ms break and cannot be changed.

- **Station active**

  The actuator is activated when the associated station is active (off-hook or loudspeaker activated). The actuator is deactivated once the associated station re-enters the idle state. A specific station must be allocated to this function.

Actuator Names

Any names (up to 16 characters) can be assigned to the actuators.

22.3.1 How to Configure an Actuator

Prerequisites

A control relay module has been inserted.

The configuration is done in Manager E (see also the online help for Manager E):

Step by Step

1) **System View**, menu **Settings** > **Auxiliary Equipment** > **Actuators**: under **Actuator list**, select the actuator to be configured.
2) **System View**, menu **Settings** > **Auxiliary Equipment** > **Actuators**: under **Actuator type**, select the actuator function.
3) **System View**, menu **Settings** > **Auxiliary Equipment** > **Actuators**: in the **Actuator name** field, enter a name of your choice for the actuator (up to 16 characters).
4) If the function is to be assigned a station, a group or all stations, select the phone number of the station or the group phone number from the **Call number** list in the **Assigned station** area.

   None must be selected for all stations.
5) If the function requires a switching time, enter the factor with which the displayed value is to be multiplied in the **Factor** field in the **Switching time** area.

   Possible display values: 100 ms and 3 s.

22.4 Sensors

Sensors are control inputs and detect a change in the state of the connected device. You can enable or disable functions of the communication system and thus support functions for monitoring, alerting, control and regulation. They are mainly used in security and building management systems (e.g., for temperature control or motion detection).

Sensors are contained in optional control relay modules. All control relay modules include four control inputs.

Possible control relay modules:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

The detailed description of these boards, including the assignments, can be found in the Service Documentation in the section on "Boards".

Sensors can enable or disable the following functions:

NOTICE: The control codes can be found the "Expert Mode" section.

- Call signaling on telephones

- Display message on system telephones
- Turning an announcement device on or off
- Answering machine control
- Automatic dialing with a predefined telephone number (internal phone number, group number or external destination call number)
- Activation of the following services for a STN (with code + STN):
  - Actuator on/off
  - Do not disturb
  - Call forwarding on/off
  - Codelock on/off
  - Send message texts
  - Withdraw message texts
  - Night service on/off
  - Ring transfer on/off
- Direct activation of the following services (only with station number):
  - Actuator on/off
  - Use speed dialing system
- Error signaling - The following are possible:
  - Output of a programmable error message (sensor name, max. 10 characters: for example, Temp Alarm) on the display of a specific system telephone (no acoustic signaling)
  - Display of calls on a specific system telephone with error message during call (destination call number)
  - Error entry in error history (entry in error memory = activated)

Destination Call Number

An associated analog port is programmable for the sensors. This port is called by the system once a setup signal has been received. The calling party then overrides this connection. A recorded announcement can be activated via an answering machine connected to this port, which informs the dialed station of the response of the sensor. An analog port programmed in this way cannot be contacted from the outside. If an external call number has been programmed for a sensor, but an analog port has not, the external connection will be established but an audible signal in relation to the response of the sensor is not transmitted. However, if necessary, the called STN can identify the origin of the call on the basis of the call number (CLIP).

Message Texts Box Control Data

Input of the control string with a maximum of 24 characters for the Phonemail system (mailbox call number). If the connection has been established, the control string is transmitted to the recorded announcement port. If a recorded announcement port is not available, the control string is transmitted to the destination.

23 Application Connectivity

Application connectivity is supported by the system, e.g., with CSTA, TAPI and Application Launcher.

23.1 CSTA

The CSTA interface enables high-performance CTI, Contact Center and Unified Communications applications, etc., to be connected to OpenScape Business.

CSTA uses the Transmission Control Protocol (TCP). A permanent connection is set up. Data packet loss is detected and automatically corrected.

Standards

The implemented CSTA protocol is based on:

- ECMA 269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- Specific extensions

Prerequisites

The use of CSTA requires either UC Booster (Card or Server) or OpenScape Business S for the system connected with CSTA applications. The login credentials for CSTA applications must be configured in the system to enable the CSTA interface automatically. External CSTA applications must use these credentials for their access.

Features

CSTA provides the following features:

- Access via Ethernet LAN (TCP/IP)
- CSTA Phase III, ASN.1 encoding
- Support for the CSTA XML protocol for certified applications
- Wide range of supported system telephones
- Network-wide monitoring and control of all resources
- Multiplexing for monitor points

Supported Devices

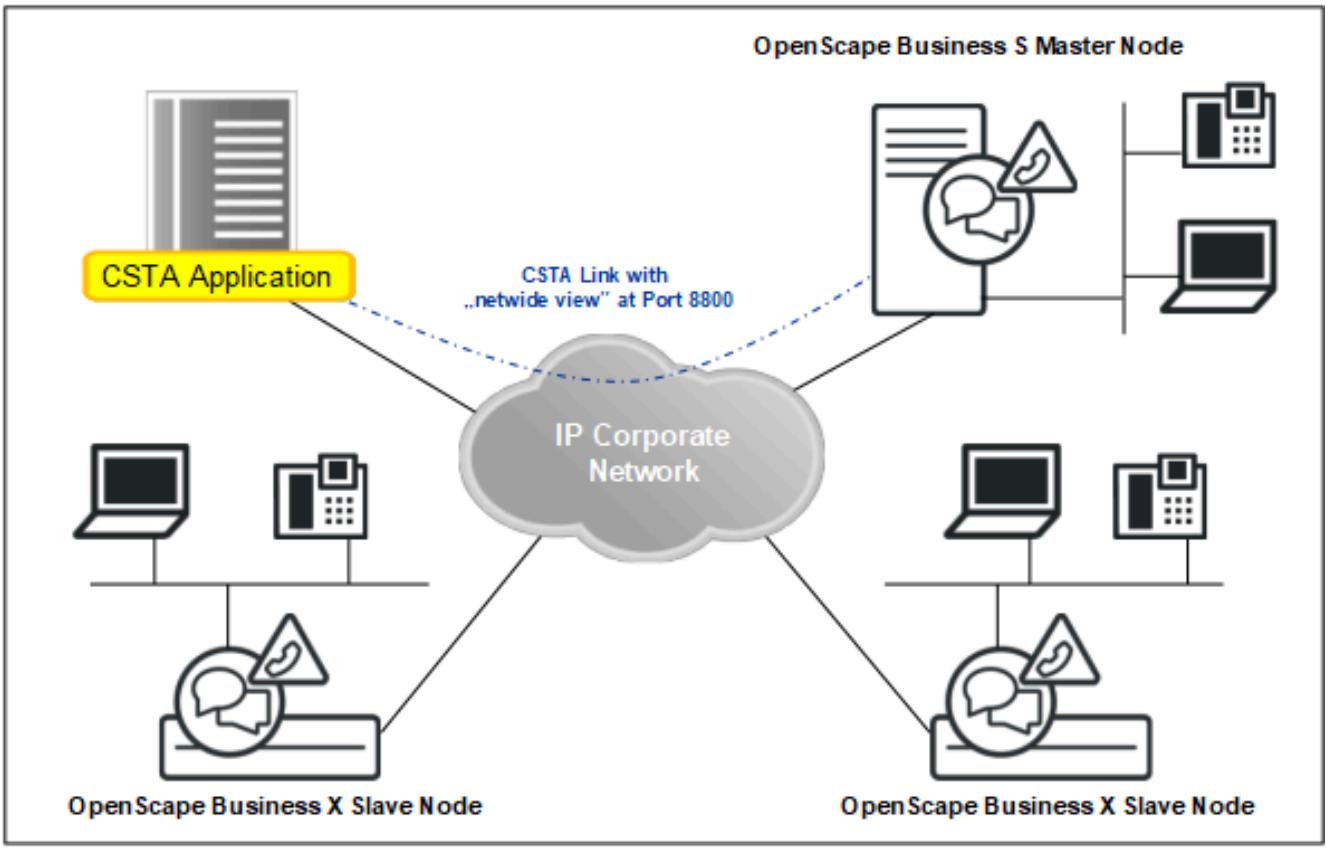
In addition to the phones supported by the system, CSTA supports the following devices:

- ITSP

  This makes it possible for Call Center applications to be used with SIP trunks
- ISDN
- Analog CO trunks
- Virtual stations
- UCD groups
- MULAPs

NOTICE: For details on features and supported devices, please refer to the CSTA Interface Manual.

Connection for network-wide view



Ports

The following port numbers are available by default:

Port	Port number	Usage
CSP	8800	any CSTA application
CMD	8900	reserved for TAPI 120 clients; regardless of the number of clients, exactly one logical CSTA link is used

External CSTA applications and TAPI 120 Service Providers must use the IP address of the UC Server or of the system with the appropriate port number in order to set up the connection. The relevant IP address is displayed in the WBM under Application Selection.

CSTA Links

By default, a CSTA link of the CSP port is available for external CSTA applications. Three other CSTA links are assigned by default to the following integrated CSTA applications or services:

- CMD (CSTA Message Dispatcher) for TAPI 120 clients at the CMD port
- DSS (Direct Station Server)
- UC Suite

If these CSTA applications or services are not needed, the corresponding CSTA links can be assigned to external CSTA applications if required.

NOTICE: A CSTA link provides the TDS service only to local devices. Customers should have a CSTA link to each node on which it is required to provide the TDS Service.

In General, CSTA applications can be connected to an OpenScape Business system via CSP, via LAS (a system component) or via PCC (an LDH component).

NOTICE: If an application is connected via CSP, it is also required to setup the credentials against CSP.

More particular:

- UC Suite, OSCC, TAPI 170 and 3rd Party (external) applications are connected via CSP

  The connection of 3rd party (external) CSTA applications that require trunk information can only be done in UC Suite mode or by querying the trunk monitoring points themselves via CSTA, in their own application.
- UC Smart is connected via LAS

Plus Products

The following flags are always enabled in the system:

- Always transmit area code with phone number
- Enhanced CSTA-CAUSE handling
- CSTA CSP signaling
- MULAP monitoring

Related concepts

Supported Phones on page 103

23.1.1 How to Change the Port Number for CSTA

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click**Basic Settings** > **Port Management**.
4) Enter the desired port number in the row for **CSP** in the input field of the **Port number** column.
5) Click on **Apply** followed by **OK**.
6) Restart the system.

Related concepts

OpenScape Business TAPI 120 on page 1110

23.1.2 How to Enable or Disable the CMD for the Use of TAPI 120

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Middleware**.
3) Click on **Middleware** > **CSTA Message Dispatcher (CMD)** in the menu tree.
4) Click on the **Settings - CSTA Message Dispatcher (CMD)** tab.
5) Select one of the following options:
   - If you want to enable the CMD, select the check box **Service will be started automatically** in the **Activation** area.
   - If you want to disable the CMD, clear the check box **Service will be started automatically** in the **Activation** area.
6) Select one of the following options:
   - If you want to use auto registration for clients, select the check box **Client auto registration enabled** in the **Auto Registration** area.
   - If you do not want to use auto registration for clients, clear the check box **Client auto registration enabled** in the **Auto Registration** area.
7) Click on **Apply**.

Related concepts

OpenScape Business TAPI 120 on page 1110

23.1.3 How to Enable or Disable the DSS Server for the Use of Network-Wide DSS Keys

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Middleware**.
3) Click on **Middleware** > **DSS Server** in the menu tree.
4) Click on the **Settings - DSS Server** tab.
5) Select one of the following options:
   - If you want to enable the DSS server, select the check box **Service will be started automatically** in the **Activation** area.
   - If you want to disable the DSS server, clear the check box **Service will be started automatically** in the **Activation** area.
6) Click on **Apply**.

23.1.4 How to Activate or Deactivate the CSP

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Middleware**.
3) Click on **Middleware** > **CSTA Message Dispatcher (CMD)** in the menu tree.
4) Click on the **Settings - CSTA Service Provider (CSP)** tab.
5) Select one of the following options:
   - If you want to enable the CSP, select the check box **Service will be started automatically** in the **Activation** area. Enter a CSTA user ID and a CSTA user password as well so that an application can use CSTA.
   - If you want to disable the CSP, clear the check box **Service will be started automatically** in the **Activation** area.

   NOTICE: If CSP is disabled, TAPI 120 (via CMD), TAPI 170, DSS Server and UC Suite will not work!
6) Click on **Apply**.

23.1.5 How to Enable or Disable the Media Extension Bridge

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Middleware**.
3) In the menu tree, click on **Middleware** > **Media Extension Bridge (MEB)**.
4) Click on the **Settings - Media Extension Bridge (MEB)** tab.
5) Select one of the following options:
   - If you want to use the Media Extension Bridge, select the check box **Service will be started automatically** in the **Activation** area.
   - If you want to release this CSTA link, clear the check box **Service will be started automatically** in the **Activation** area.
6) Click on **Apply**.

23.2 OpenScape Business TAPI 120/170

OpenScape Business TAPI 120 and OpenScape Business TAPI 170, in addition to CallBridge Collection, are two TAPI Service Providers (TSPs) that are optimized for the system architecture and network topology of OpenScape Business. These TSPs provide the Microsoft TAPI interface to TAPI-based applications for the connection to the OpenScape Business communication system.

The connection to OpenScape Business takes place exclusively via the LAN. Additional hardware and software components such as the CSTA Message Dispatcher (CMD) or CSTA Service Provider (CSP) are no longer required for operation with OpenScape Business. The licensing is station based and does not distinguish between OpenScape Business TAPI 120 or TAPI 170 stations. The licensing requirement begins with the first TAPI station.

The choice of the appropriate TAPI Service Provider essentially depends on the number of client PCs to be connected with TAPI applications as well as the existing IT infrastructure and the telephones used.

- **CallBridge Collection**

  is used as a traditional first-party TAPI Service Provider on system telephones that have a LAN or USB interface. It is suitable for installations with just a few PCs. A LAN is not necessary for the operation of the CallBridge Collection. The CallBridge Collection is installed on each PC that is running a TAPI application. Analog, Cordless and system telephones without USB/IP interfaces are not supported.

  TAPI connections via the CallBridge Collection are not licensed.
- **OpenScape Business TAPI 120**

  is used as the preferred first-party TAPI Service Provider in Microsoft networks with or without a domain controller when analog, Cordless and system telephones without USB/IP interface are also to be operated in conjunction with the TAPI application. The TAPI 120 Service Provider is installed on each PC client that is running a TAPI application.

  TAPI connections via OpenScape Business TAPI 120 are subject to licensing within OpenScape Business. To connect to OpenScape Business, depending on the operating mode or connection type, one CSTA link or a link to the Web Services Interface is required, regardless of how many TAPI 120 clients are being operated. The scope of functionality on the TAPI side depends on the operating mode and type of connection.
- **OpenScape Business TAPI 170**

  is a classic "third-party" TAPI Service Provider. It is installed on a server on the LAN and connected centrally to the OpenScape Business System. TAPI 170 can be used as an alternative to TAPI 120 if there is a domain controller in the Microsoft network. When using the so-called remote TAPI function, it is not necessary to install the TAPI Service Provider on the client PCs. This offers significant time savings in installations with many client PCs. Please note, however, that the use of OpenScape Business TAPI 170 is mandatory in the following constellations:

  – Connection of TAPI stations to networked OpenScape Business systems when the TAPI stations are located in different nodes.
  – Connection to TAPI applications running on a terminal server.
  – Connection to server-based TAPI applications.

  TAPI connections via OpenScape Business TAPI 170 are subject to licensing within OpenScape Business. To connect to OpenScape Business, one CSTA link is required, regardless of how many TAPI 170 stations are being operated.

23.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 is a first party telephony service provider that supports the Microsoft TAPI V2.1 functionality. OpenScape Business TAPI 120 enables Windows-based CTI applications to monitor and control a system telephone connected to OpenScape Business.

OpenScape Business TAPI 120 can be alternatively connected to OpenScape Business via the CSTA interface (CSTA mode) or the Web Services Interface (UC Smart mode). A mixed operation using both interfaces to the system is not possible. If a UC Booster Card is plugged into the OpenScape Business system or if a UC Booster Server has been enabled, TAPI 120 can only be operated in the CSTA mode. The system requirements, the maximum number of TAPI stations and the scope of functionality on the TAPI side depend on the operating modes.

OpenScape Business TAPI 120 Connections

The OpenScape Business TAPI 120 software is installed on a Microsoft Windows client PC. The connection to the OpenScape Business System is made via LAN. A physical connection between the Windows PC and the phone is not required.

- **TAPI 120 CSTA mode**

  All TAPI 120 client PCs are connected to the same CSTA link of OpenScape Business. OpenScape Business internally multiplexes all TAPI 120 connections.

  TAPI 120 in CSTA mode supports OpenScape Business X3/X5/X8 and OpenScape Business S.

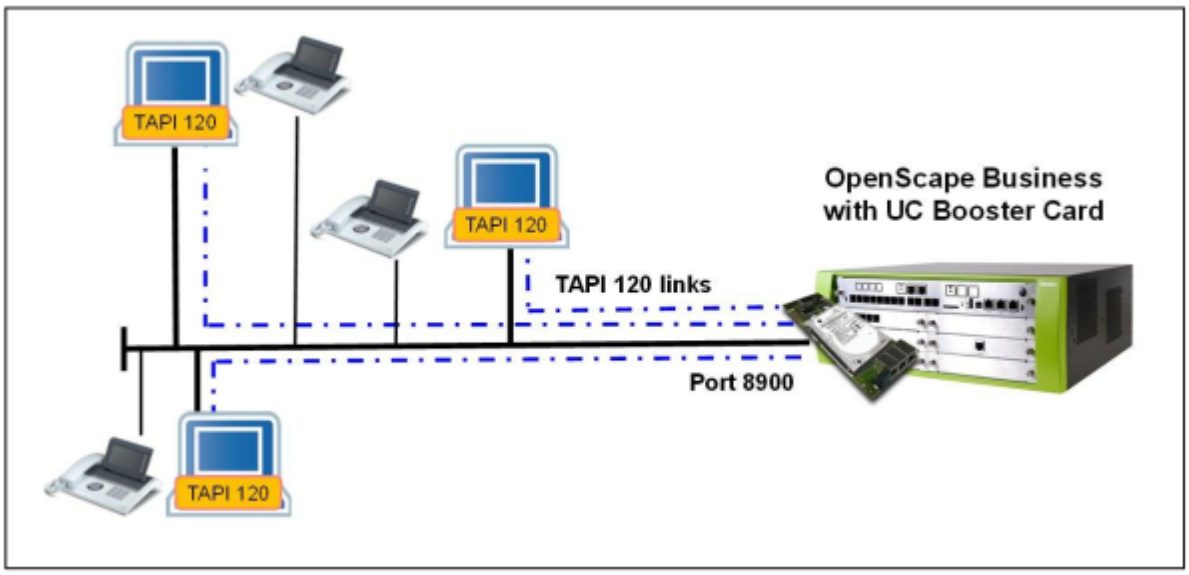


Figure 11: TAPI 120 in CSTA Mode with OpenScape Business X5R and UC Booster Card

- **TAPI 120 UC Smart mode**

  All TAPI 120 client PCs are connected to the mainboard of OpenScape Business via the LAN and Web Server interface. OpenScape Business internally multiplexes all TAPI 120 connections.

  TAPI 120 in CSTA mode supports OpenScape Business X1/X3/X5/X8.

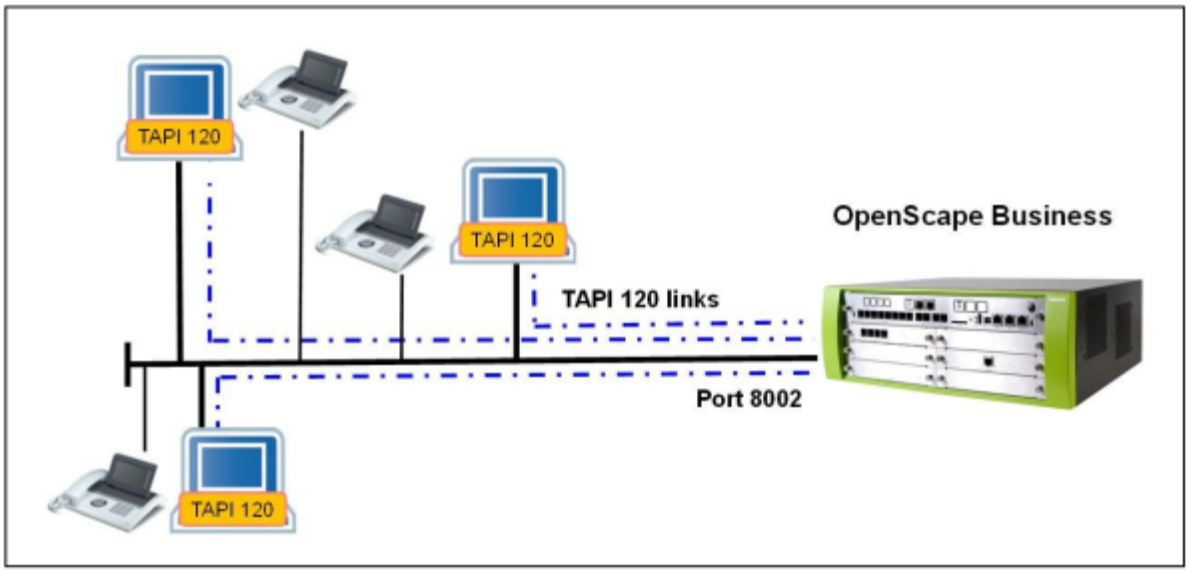


Figure 12: TAPI 120 in UC Smart Mode with OpenScape Business X5R

Features

The following features are supported:

Feature	TAPI 120 CSTA	TAPI 120 UC Smart
Central first-party TAPI Service Provider connected via a LAN	X	X
Compatible with the Microsoft TAPI 2.1 Standard	X	X
Connection to standalone OpenScape Business system	X	X
Support for the OpenScape Business CTI firewall	X	-
Features supported via TAPI		
Call signaling of incoming and outgoing calls with identification of call numbers and origin of call	X	X
Additional information in the call signaling for redirected calls	X	X
Answering internal and external calls	X	X
Controlled connection setup to internal and external called parties	X	X
Manual dialing / DTMF suffix dialing	X	X
Release existing calls	X	X

Feature	TAPI 120 CSTA	TAPI 120 UC Smart
Set up consultation call to internal and external parties	X	X
Alternate (toggle/connect)	X	X
Screened call transfer	X	X
Screened call transfer with subsequent dialing of the consultation destination (one-step transfer)	X	X
Unscreened call transfer (blind transfer)	X	-
Set and delete call forwarding	X	X
Set and clear DND	X	X
Initiate conference	X	-
Expand conference	X	-
Forward incoming call	X	-
Directed pickup (call pickup)	X	-
Group signaling and group pickup	X	-
Park existing calls	X	-
Resume parked calls	X	-
Place existing calls on hold manually	X	-
Resume calls placed on hold manually	X	-
Set callback	X	-
Support for code-driven functions	X	-
Call-related data exchange between TAPI applications	X	-
Control of keys on system telephones (HFA)	X	-
Control of microphone gain on system telephones (HFA)	X	-
Control/select use of handset/loudspeaker/headset for system telephones (HFA)	X	-
Control volume of handset/loudspeaker/headset/ keyboard on system telephones (HFA)	X	-
Access to optiPoint/OpenStage displays and LEDs (with limitation to 50 active displays per system)	X	-

Maximum Values

The maximum number of TAPI 120 client PCs that can be connected to OpenScape Business depends on the model (see Expansion Levels Available through Sales).

Released Operating Systems

The currently released operating systems for the Microsoft Windows Server, the Terminal Server and the remote client PC are listed in the latest Sales Information.

Only Microsoft Windows operating systems can be used in conjunction with TAPI 120.

For installations on terminal servers, OpenScape Business TAPI 170 must be used instead of OpenScape Business TAPI 120.

Licensing

The use of OpenScape Business TAPI 120 is licensed on a subscriber basis. The TAPI licenses are managed within the OpenScape Business system and can be used for both modes of TAPI 120. When using the MULAP feature, a TAPI license is required for each station within the MULAP.

NOTICE: No UC User licenses are required for TAPI 120 in UC Smart mode.

Software Provisioning

The OpenScape Business TAPI 120 software is supplied on a separate data medium. It is not part of the OpenScape Business system software.

Hardware Requirements

The PC must comply with at least the system requirements specified by Microsoft for the operating system used as well as the requirements of the TAPI application. In addition, an Ethernet LAN interface is required.

- For TAPI 120 CSTA

  One CSTA link of OpenScape Business is required, regardless of how many TAPI 120 clients are connected. An OpenScape UC Business Booster (Card or Server) is mandatory for this purpose.
- For TAPI 120 UC Smart

  The Web Services interface is required. There must be no OpenScape UC Business Booster (Card or Server) present in/at the system.

Supported Devices

The supported devices as well as the supported features on these devices depend on the CSTA or the WSI functionality of the OpenScape Business system being used. This information is contained in the OpenScape Business Sales Information.

Default IP Port / IP Address Occupied by TAPI 120

In the TAPI 120 CSTA operating mode, the CSTA link to OpenScape Business occupies IP port 8900.

In the TAPI 120 UC Smart operating mode, the WSI link to OpenScape Business occupies IP port 8802 for an encrypted connection (HTTPS) or 8801 for an unencrypted connection (HTTP).

In the TAPI 120 configuration, the IP address of the OpenScape Business system must be entered in accordance with the operating mode. This IP address is displayed in the WBM under **Application Selection**.

Related tasks

How to Change the Port Number for CSTA on page 1106
How to Enable or Disable the CMD for the Use of TAPI 120 on page 1107

23.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 is a third party telephony service provider that supports the Microsoft TAPI V2.1 functionality. TAPI 170 enables Microsoft Windows-based CTI applications to concurrently monitor and control telephones connected to OpenScape Business.

Features

OpenScape Business TAPI 170 provides the following features:

- Centrally connected third-party TAPI Service Provider
- Compatible with the Microsoft TAPI 2.1 Standard
- Telephony functions are available on each connected PC client via the TAPI 2.1 client/server architecture
- No additional TSP client software is required
- Supported telephony features:
  - Selection or dialing of incoming/outgoing calls from the PC
  - Transmission of incoming call number, if signaled
  - Consultation and transfer
  - Toggle/Connect
  - Conferencing
  - Call forwarding
  - Forwarding callers
  - Answering a call through the application
  - Initiating a call through the application
  - Blind/Supervised transfer (also called "transfer before answer / consultation transfer")
  - Transmission of feature codes
  - Monitoring of the phone (call states, failure, etc.)
  - Provision of an ACD interface
  - Monitoring/access to keypad for system telephones (HFA)
  - Control of display/LED for system telephones (HFA)
  - Connection to standalone and networked OpenScape Business systems
  - Support for MULAP members/station numbers

OpenScape Business TAPI 170 Connections

The OpenScape Business TAPI 170 software is installed on a Microsoft Windows server on the network. The connection to OpenScape Business occurs via a CSTA link. A physical connection between the Windows PC and the phone is not required. OpenScape Business TAPI 170 can be set up in different operating modes on standalone systems or in the OpenScape

Business network. The TAPI server and clients must be managed by the same network domain controller.

- **Connecting Server-based TAPI Applications to OpenScape Business using TAPI 170**

  The server applications and the TAPI 170 software are installed on the so-called "Telephony Server" in the network. The server applications provide their associated clients in the network with telephony features for the stations that are configured within OpenScape Business TAPI 170. The TAPI 170 software is connected to the CSTA interface of OpenScape Business over the LAN. For this connection, one CSTA link of OpenScape Business as well as one TAPI license for each configured TAPI station are required.

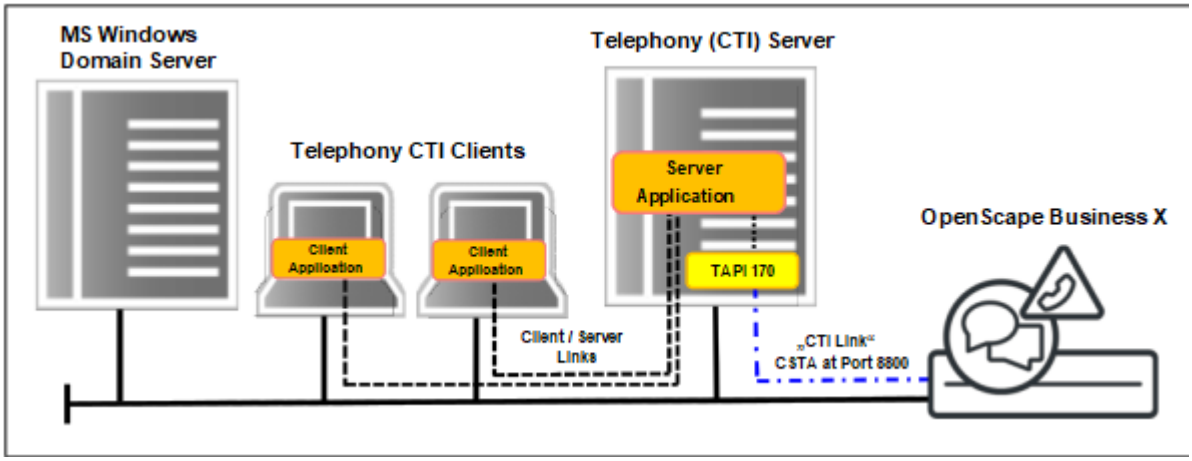


Figure 13: Server-Based TAPI Application via TAPI 170 to OpenScape Business

- **Connecting Client-based TAPI Applications to OpenScape Business using TAPI 170 with the "Remote TAPI" Function**

  In this scenario, the OpenScape Business TAPI 170 software is installed on a server on the network. On the client PCs with the TAPI applications, the so-called "Remote TAPI" function is enabled, via which the TAPI application on the client communicates with the TAPI 170 software on the server. No TAPI 170 software needs to be installed on the client for this purpose.
  The TAPI 170 software is connected to the CSTA interface of OpenScape Business over the LAN. For this connection, one CSTA link of OpenScape

Business as well as one TAPI license for each configured TAPI station are required.

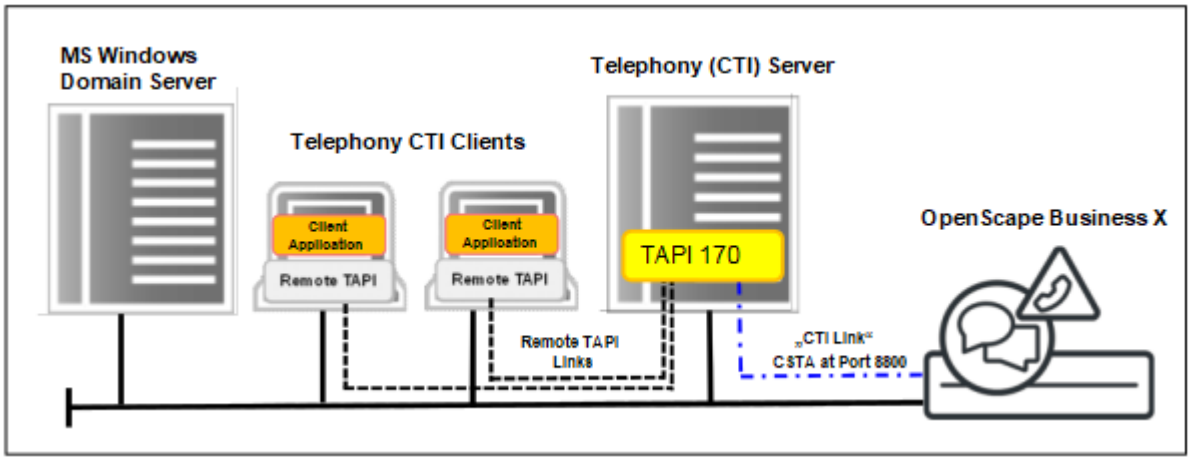


Figure 14: Client-Based TAPI Application via "Remote TAPI" to OpenScape Business

- **Connecting Terminal Server-based TAPI Applications to OpenScape Business using TAPI 170**

  In this scenario, the client-based TAPI applications are installed on one or more terminal servers. In this case, the TAPI 170 software is also installed on the terminal server. In the case of a cluster consisting of multiple terminal servers, the TAPI 170 software must be installed on each terminal server in the cluster. Each instance of the installed TAPI 170 software is connected to OpenScape Business over the LAN. For each instance of the TAPI 170 software installed on a terminal server, one CSTA link of OpenScape Business is required. In addition, a TAPI license is also required for each configured TAPI station.

  The maximum possible number of OpenScape Business TAPI 170 servers in conjunction with OpenScape Business must not be exceeded.

  NOTICE: The number of terminal servers that can be operated in the cluster is limited to the number of free CSTA links available within OpenScape Business for connecting the TAPI 170 software. The maximum number of possible

connections is reduced if the CSTA links of OpenScape Business are used by other CSTA applications.

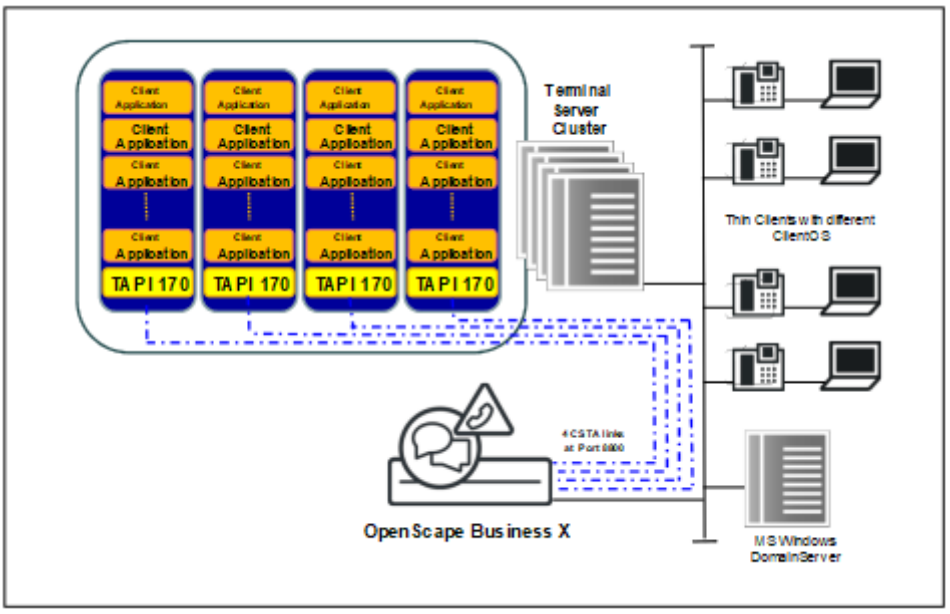


Figure 15: Client-Based TAPI Applications on Terminal Server to OpenScape Business

- **Connecting TAPI 170 to Networked OpenScape Business Systems**

  For networked OpenScape Business systems, the TAPI 170 software is installed on one server, which is connected via the LAN to the CSTA interface of the master node. This connection is independent of the previously mentioned operating modes of the TAPI 170 Service Provider (remote TAPI or server-based connection). To implement this connection, one CSTA link of the OpenScape Business master node as well as one TAPI license for each configured TAPI station are required.

  NOTICE: Via the master node, the TAPI 170 receives network-wide access to all stations in the network. If the TAPI 170 is connected to a slave node instead of the master node, TAPI 170 can access only the stations of the slave node. When using multiple TAPI 170 in a terminal server cluster,

one CSTA link to the master node is required for each TAPI 170.

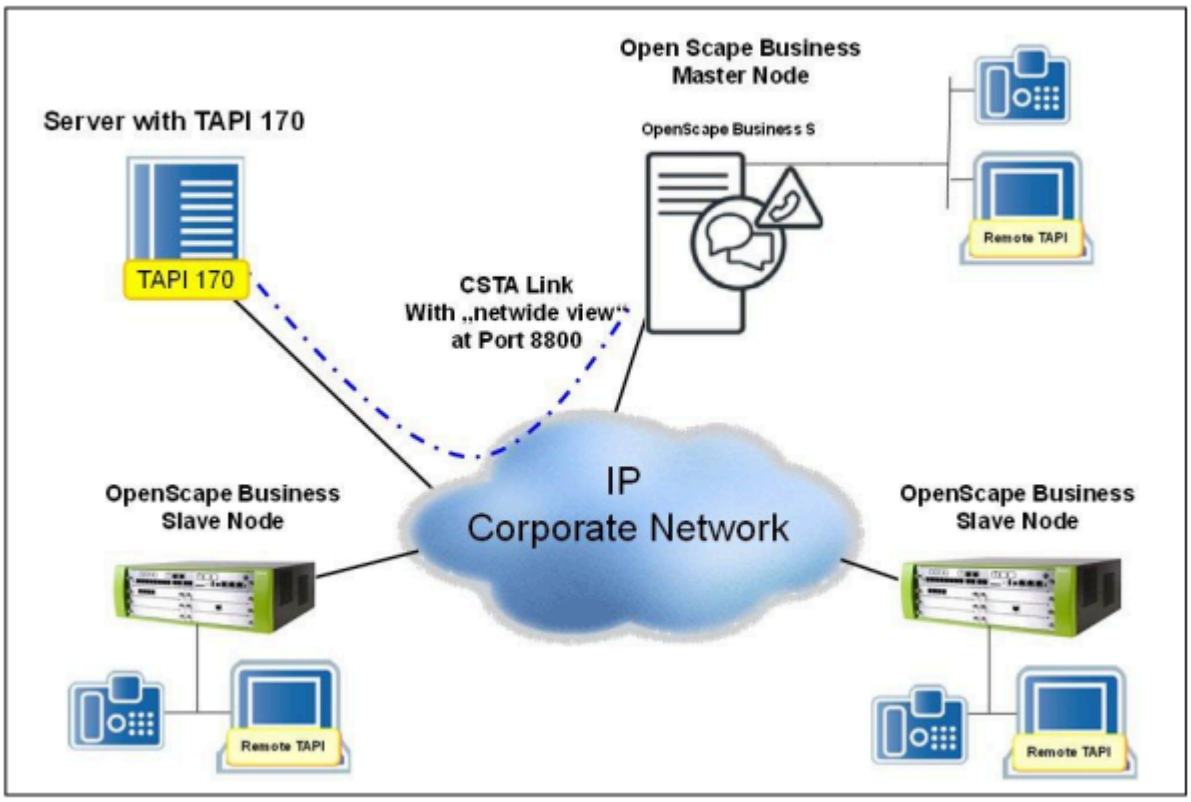


Figure 16: Connecting TAPI 170 to Networked OpenScape Business Systems

Capacity Limits

The maximum number of TAPI 170 client PCs that can be connected to OpenScape Business depends on the model. More information on this can be found in section 1.3.9.4

Released Operating Systems

The currently released operating systems for the Microsoft Windows Server, the Terminal Server and the remote client PC are listed in the latest Sales Information.

Only Microsoft Windows operating systems can be used in conjunction with TAPI 170.

In addition to the license for the server operating system, the Microsoft licensing model requires Microsoft device or User CALs corresponding to the number required for the planned expansion. These CALs are not included in the delivery of OpenScape Business TAPI 170 and must be purchased separately. Under certain conditions specified by Microsoft, a "Windows Server for embedded systems" with the so-called "embedded Telco license" can be used for OpenScape Business TAPI 170.

Licensing

The use of OpenScape Business TAPI 170 is licensed on a subscriber basis. The licenses are managed within the OpenScape Business system. When using the MULAP feature, a TAPI license is required for each station within the MULAP.

Software Provisioning

The OpenScape Business TAPI 170 software is supplied on a separate data medium. It is not part of the OpenScape Business system software.

Hardware Requirements

In order to connect to OpenScape Business TAPI 170, one CSTA link of OpenScape Office is required, regardless of how many TAPI 170 clients are connected. This also applies to networked OpenScape Business systems.

The PC must comply with at least the system requirements specified by Microsoft for the operating system used, provided that no further software applications other than TAPI 170 are being operated. In addition, an Ethernet LAN interface is required.

Supported Devices

The supported devices as well as the supported features on these devices depend on the CSTA or the WSI functionality of the OpenScape Business system being used. This information is contained in the OpenScape Business Sales Information.

23.3 Web Services Interface

The integrated web services interface enables the monitoring and control of telephony resources in a system with UC users.

Features

The web services interface provides the following features:

- Access via Ethernet LAN (TCP/IP)
- Support for HTTP and HTTPS
- Support for individual systems
- User-oriented, clearly structured functions for:
  - Call control
  - Device control
  - Monitoring devices
  - Directories
  - Journals of users
  - Presence status of users

NOTICE: Depending on the WSI (Web Services Interface) client type, station flag Associated Services must be activated in order to enable execution of some of the WSI commands.

Web Server WebSessions

The number of available web server sessions is common to all relevant applications (e.g., myPortal to go, Application Launcher, optiClient Attendant (Server) and optiClient BLF.

Internal Monitor Points

The internal monitor points are independent of the monitor points of the CSTA interface. If several applications monitor the same UC user via the web services interface, only a single internal monitor point is used by the web server for this purpose.

Ports

The following port numbers are available:

Port	Protocol
8801	HTTP (unencrypted)
8802	HTTPS (encrypted)

23.4 Open Directory Service

Open Directory Service (ODS) is an open, integrated, LDAP based directory service. It acts as a meta-directory service, aggregating the results from different internal and external directory sources via a single interface. Open Directory Service can be accessed by different types of clients, applications and communication devices in a company.

The Open Directory Service performs two functions:

1) It provides access to additional contact data from external sources via SQL or ODBC data access to databases in the customer network which contain directory data

2) It exposes both internal and external directories to clients, communication devices and applications.

Open Directory Service is disabled by default. When activating it, please also make sure that firewalls are open for the LDAP protocol on port TCP/389.

Open Directory Service on different variants of OpenScape Business

Open Directory Service is offered with different features dependent on the OpenScape Business platform:

- OpenScape Business S, OpenScape Business X V3 Advanced mainboards, Booster Server or Booster card:

  Full functionality is offered, so that both internal and external data sources can be used
- OpenScape Business X V3 Basic mainboards:

  The functionality is limited to the internal default data sources.
- OpenScape Business X V2 mainboards:

  A Booster Card or Booster Server is required to utilize Open Directory Service.

To connect to Open Directory Service via the LDAP protocol, please use the IP address shown in the Admin Portal:

- On the right side of OpenScape Business Assistant homepage, under **Applications**.
- On the **Application Selection** page of the **Initial Installation** wizard, under **Setup** > **Basic Installation**.

Internal Data Sources

The following internal data sources are available by default in the Open Directory Service:

- External directory
- Internal directory
- Central speed-dial numbers

For these internal data sources, the field names are permanently mapped to the data schema of the Open Directory Service.

These internal data sources cannot be deleted or modified. To expose internal data sources via ODS, an "OpenScape Business OpenDirectory Base" license is required.

External Data Sources

As an administrator, you can integrate contact information from the following types of databases as data sources for read-only access via SQL or ODBC.

- Data sources with built in drivers (Microsoft SQL Server, PostgreSQL, Sybase SQL).
- Data sources without built in drivers, require an installed and configured ODBC Bridge Server on the ODS client (downloadable via the WBM under **Service Center** > **Software**).

NOTICE: For a successful connectivity, it is necessary to define a value (the value can be different from the name of the data source, but the field cannot be empty) in the **Description** field. In case of ODBC bridge data source for Access, Firebird, Excel and Oracle, please add the name of the data source, "access", "firebird", "excel", "oracle" respectively, as the value of the **Description** field.

NOTICE: For Microsoft Excel - ODS database integration, only *.xsl* (but not *.xlsx*) file format is supported. In recent MS Office releases, avoid editing/saving the excel files not to break the file's encoding. Additionally, a specific ODBC Bridge driver for Microsoft Excel is required.

To access external data sources from ODS, one "OpenScape Business OpenDirectory Connector" license is required, per connected data source.

Maximum number of different types of databases: 3

Maximum number of external data sources: 4

Make sure that the Open Directory Service is authorized to access the external data source. Contact the responsible database administrator in advance to

ensure that this is the case. A separate user may need to be added in the external data source for access by the system.

External data sources can be used in the context of both directory searches and the resolution of call numbers into names.

You can configure direct access to a database table from an external data source or a custom SQL query for the data source.

Any column which serves as an ID must contain unique and not null/not empty values. Use the UNIQUE or PRIMARY KEY property to ensure that this is the case.

In cases where external databases are integrated, the following restrictions apply:

- The special characters ´[]'" are not supported by the ODS in table names and column names.
- The column types "nchar" and "nvarchar" are not supported by the ODS.
- The intermediate blank space characters (at least in the last 4-5 digits) are not supported by the ODS for phone data.

Custom SQL Queries for External Data Sources

Custom SQL queries also support related tables, e.g.:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON
users.id = phonenumbers.uid;
```

The data structure must be of the type 1:1 or n:1, i.e., each record can have only a single row.

Access via custom SQL queries can sometimes run much slower than direct access to a database table.

Custom SQL queries with potential security risks are not executed, for example:

- Modifying data
- Stopping the SQL server
- Running programs via the SQL server
- Changing user rights

Custom SQL queries with the following SQL commands are therefore not executed:

- CHECKPOINT
- CLOSE
- CLUSTER
- COMMIT
- COPY
- CREATE
- DEALLOCTAE
- DECLARE
- DELETE
- DISCARD
- DO
- DROP
- END
- EXECUTE
- EXPLAIN

- FETCH
- GRANT
- INSERT
- LOAD
- LOCK
- MOVE
- PREPARE
- REASSIGN OWNED
- REINDEX
- RELEASE SAVEPOINT
- RESET
- REVOKE
- SAVEPOINT
- SECURITY LABEL
- SELECT INTO
- SET
- SHOW
- START TRANSACTION
- TRUNCATE
- UNLISTEN
- UPDATE
- VACUUM
- VALUES

Field Mapping for Data Sources

For these data sources, you can customize the mapping of field names to the data schema of the Open Directory Service. You can assign each field in the data schema of the Open Directory Service to no more than one field of the external data source. However, you can assign a field of the external data source to multiple fields in the data schema of the Open Directory Service.

LDAP Data Output Mappings

An LDAP data output mapping determines which of the fields in the data schema of the Open Directory Service are to be output via LDAP, e.g., for specific LDAP clients or for different groups of subscribers who do not want to see all the details, but only a defined subset.

The LDAP data output mapping **web** is available by default and cannot be deleted or changed. All fields of the data schema in the Open Directory Service are permanently assigned to the LDAP output in it. You can also configure other LDAP data output mappings.

LDAP clients can access a specific LDAP data output mapping via the dc parameter in the LDAP login, for example: `dc=web`.

Normalization of Phone Numbers in the Canonical Format

For each data source, you can configure the normalization of phone numbers in the canonical format. During this process, blanks, parentheses, hyphens and commas are removed. This is required to correctly identify the caller's name and for desktop dialing. You should not skip the normalization, unless the phone numbers used in the data source are already present in canonical format. You can have the normalization-related values such as the area code, etc.,

entered automatically from the system. If the external data source is located at a different site than the system, you may need to adjust these values.

Status of Data Sources

The status display under **OpenDirectory** > **Data Sources** has the following significance:

Color	Status
green	active
red	ODBC and LDAP is not OK, wrong configuration or data source unavailable
yellow	LDAP not ok: restart the Open Directory Service
gray	Configuration incomplete

Provision of directories

The following types of clients, communication devices and applications can use the directories provided by the Open Directory Service:

- UC Clients
- Application Launcher
- System Directory
- OpenStage with local LDAP support
- DECT IP phones (via LDAP)
- SIP phones (via LDAP)
- Applications, e.g., CRM Suites such as Microsoft Dynamics CRM (via LDAP, ODBC or OpenLDAP CSV export)

Open Directory Service can identify in the search results the data source from which a hit is obtained.

Related concepts

Prerequisites for Application Launcher on page 1133

23.4.1 How to Enable or Disable the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.
3) Click on **Open Directory** > **Basic Settings** in the menu tree.
4) Select one of the following options:
   - If you want to enable the Open Directory Service, select the **Active** check box.
   - If you want to disable the Open Directory Service, clear the **Active** check box.

5) Click on **Save**.
6) Click on **OK**.
7) Click on **OK**.

23.4.2 How to Restart the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Open Directory Service is enabled.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.
3) Click on **Open Directory** > **Maintenance** in the menu tree.
4) Click on **Restart**.
5) Click on **OK**.

23.4.3 How to Configure the Password for Access to the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Follow these steps to set the password with which clients, communication devices and applications can access the Open Directory Service.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.
3) Click on **Open Directory** > **Basic Settings** in the menu tree.
4) Enter the desired **LDAP Password**.
5) Click on **Save**.
6) Click on **OK**.

23.4.4 How to Configure the ODBC to ODBC Bridge Server

Prerequisites

The ODBC Bridge Server was downloaded from the WBM under **Service Center** > **Software** and installed on a Windows PC (32 bit or 64 bit) with data sources that can access relational or non relational databases. The ODBC Bridge Server is required for ODBC drivers to access the data source.

NOTICE:

Due to recent Windows 10 / Windows Server updates by Microsoft, the ODBC interface of the operating system has been changed and therefore only 32-bit drivers are supported by the ODBC to ODBC Bridge. It is strongly recommended to use 32bit ODBC drivers to connect to ODBC data sources for time being.

This is a temporary restriction.

The data source must be configured as a DSN on the ODS client via the ODBC data source administration.

The user name and password of the data source are known.

The configuration of the ODBC Bridge Server is described here for the English user interface. The configuration can, of course, also be performed using a different interface language (**Server Manager** > **Language** tab).

Step by Step

1) Right click on the ODBC Bridge Server icon in the tray bar and select the menu item **Settings**.

2) Define the general server settings:

a) Click on the **Server Settings** tab.

b) Under **Connection Settings**, select the IP address under which the ODBC Bridge Server is to be accessible to the ODBC client (OpenScape Business) from the **Network Interface** drop-down list.

This IP address must be entered for the ODS configuration in the WBM of OpenScape Business.

c) Under **Port**, enter the port through which the queries of the ODBC client (OpenScape Business) are to be received.

This port must be entered for the ODS configuration in the WBM of OpenScape Business.

d) If the service is stopped, you can activate the **Service Status** by setting it to **On** under **Service Control**, or by selecting **Start service** in the tray bar.

e) If the service is connected, you can disable the **Service Status** by setting it to **Off** or by selecting **Stop service** in the tray bar.

f) Under **Network Settings**, you can enable the encryption by setting it to **On**.

g) Under **Network Settings**, enter the maximum number of simultaneous connections to ODBC clients (minimum: 1, maximum: 20) in the **Max Connections** field.

h) Click **Save Settings**.

NOTICE: After saving the settings, a service restart is required.

3) Create a user for the ODBC client access to the data source:
   a) Click on the **Role Management** tab.
   b) Click **Add User**.
   c) Assign a user name for the ODBC client in the **Username** field.
   d) Enter a password for the ODBC client in the **Password** and the **Re-Enter Password** fields.

      The same user details must be entered for the ODS configuration in the WBM of OpenScape Business.
   e) Select the DSN to which the ODBC client should have access, by checking the box under the **Access** column.
   f) Enter the **DB Username** and **Password** if required.
   g) Click **Save Settings**.
4) Click on the **Monitoring** tab to monitor the connections. The following details are displayed:
   - The installed ODBC drivers' names and versions.
   - The name and the IP address of the ODS client, the last active connection time and the total active connection time.
   - The available ODBC datasources (via the **Open Windows Datasource Administrator** link).
5) Click on the **Logs** tab to enable the creation of log files and set which trace levels should be logged:
   a) Enable logging by setting it to **On**.
   b) Select the **Log Level**: **Everything** for all logs, **Normal** for service logs or only **Warnings and Errors**.
   c) Select the log type from the drop-down list. You can select to view the logs folder or the log console.
6) Click on the **Appearance** tab to change the appearance:
   a) Select a theme (dark or light).
   b) Select a style.
   c) Set the desired language.
   d) Select whether the service should run automatically on startup.
   e) Select whether the service can be minimized to tray.
7) Click on the **About** tab to view the service details and the available updates.

   NOTICE: If a new version is available, click **Install** to run the update.
8) Select **Exit** in the tray bar, to close the service configuration.

23.4.5 How to Add an External Data Source for the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

The access data of the external database is available.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.

3) Click on **Data Sources** in the menu tree.
4) Click **Add**.
5) Click on the **Database** tab.
6) Enter the **Name** of the data source.
7) Enter a **Description** for the data source.
8) If you want to add an SQL database:
   a) Select the type **PostgreSQL** or **Microsoft SQL Server, Sybase SQL** or **ODBC Bridge** from the **ODBC driver** drop-down list.
   b) Enter the PV4 address of the database under **Database Server Address**.
   c) Specify the **Database Server Port**.
   d) Enter the **Database name** in the correct case.
   e) Enter the **Database login** in the correct case.
   f) Enter the **Database password** in the correct case.
   g) If you selected the type **Microsoft SQL Server, Sybase SQL** in the **ODBC driver** drop-down list, enter the **TDS Protocol Version** as well.
9) If you want to add a non-SQL database:
   a) Select the type **ODBC Bridge** from the **ODBC Driver** drop-down list.
   b) Enter the IPv4 address of the database in the **ODBC Bridge Server Address** field.
   c) Enter the **ODBC Bridge Server Port**.
   d) Enter the **ODBC Bridge Remote DSN**
   e) Enter the correct case-sensitive **ODBC Bridge Login**.
   f) Enter the correct case-sensitive **ODBC Bridge Password**.
10) Click on **Check database access** to test the access.
11) Click **Save**.
12) Click on the **Data Access** tab.
13) If you want to use a database table:
   a) Click on **Simple selection - access one table**.
   b) Click on **Query database tables** and select the desired table in the **Database tables** list.

NOTICE: This functionality is not supported for some datasources (e.g. Oracle). If so please provide the table name manually.

---

   c) Click on **Preview database table** and navigate through the records in the preview with the aid of the appropriate buttons.
14) If you want to use a custom SQL query:
   a) Click on **Self-defined SQL query**.
   b) Enter the SQL query in the **Define SQL query** field.

NOTICE: When defining a new datasource with an SQL statement you should formulate the query in a way that ensures that the record IDs will be constant. You have to utilize the ID attributes included in the respective tables instead of computing IDs when the query runs. Please avoid any statement such as "SELECT ROW_NUMBER() OVER As ID" that creates IDs when the query is executed and that will deliver different IDs

depending on sorting and amount of records. In case of uniting tables with overlapping ID ranges with UNION ALL, mitigate the risk of duplicate IDs by incrementing the existing table IDs with a different number for each table to be united (eg "SELECT (table2.ID+1000) AS ID").

c) Click on **Preview query results** and navigate through the records in the preview with the aid of the appropriate buttons.

15) Click on the **Field mappings** tab.

NOTICE: All columns of the selected table and all columns returned by the custom SQL queries are available for field mappings.

16) Click on **Add Field Mapping**.

17) Select the field of each external data source in the drop-down list on the left and then select the corresponding field to be mapped in the data schema of the Open Directory Service via the drop-down list on the right in the same row. For verification purposes, a preview of the relevant records appears on the right, which you can navigate by using the appropriate buttons.

NOTICE: The **Unique Identifier** field must be mapped to a field in the external data source that is unique.

18) If you want to remove a row of field assignments, click on the trash icon on the left.

19) Click on the **Number conversion** tab.

a) Select the **Active** check box.

b) Click on **Query System Settings**.

c) If the external database is located at a different site than the system Enter the **Country Code**, **Local Area CodeCentral Office Number**, **National Prefix**, **Maximum internal number length**

d) Select one of the following options:

- If you want to remove any dial-out prefix (CO code) that may be present in the external data source, select the **Remove dialout prefix** check box.

- If you do not want to remove the dial-out prefix, clear the **Remove dialout prefix** check box.

20) Click **Save**.

21) Click **OK**.

Next steps

Restart the Open Directory Service for the change to take effect.

Preview the LDAP search result.

23.4.6 How to Preview LDAP Search Results for the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Follow these steps to check whether an LDAP search result of the Open Directory Service returns records in the desired form and with the correct number format.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.
3) Click in the menu tree under **Open Directory** > **OpenScape Business Users** > **Data Sources** on the desired data source.
4) Click on the **LDAP test** tab.
5) Click on **Run test**. The preview of the search result will appear under **LDAP Search Result**.

NOTICE: Default response limit of OpenLDAP is 500 entries. Open Directory Service (ODS) backend engine also imposes a limit of 500 entries for each datasource.

LDAP test functionality of Open Directory Service (ODS) performs a search query which reaches the limit of 500 entries. The purpose of the LDAP test option is not the retrieval of the results but to validate that LDAP connectivity is proper.

Therefore, if more than 500 records exist, additions and modifications to LDAP data may not be reflected over the WBM after executing an LDAP Test.

23.4.7 How to Delete an External Data Source for the Open Directory Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **Open Directory Service**.
3) Click on **Open Directory** > **Data Sources** in the menu tree.
4) Click on the relevant data source in the workspace.
5) Click on **Delete**.
6) Click on **OK**.

Next steps

Restart the Open Directory Service for the change to take effect.

23.5 Active Directory Integration Service

Active Directory is a Microsoft directory service for domain networks. With the offered Active Directory Integration Service, OpenScape Business can read the Active Directory database and synchronize users to its own user database to simplify user administration and reduce configuration efforts.

Prerequisites

For the Active Directory Intregration Service synchronization to take place, the following prerequisites must be satisfied:

- There is Active Directory Microsoft Server deployed by the customer
- The Active Directory is used as a single point of configuration for employee data, and especially user data. The following fields will be mapped between Active Directory and OpenScape Business:
  - first name
  - last name
  - display name
- Only this Active Directory is used to add, change, or delete data of employees.
- All Active Directory changes are expected to automatically take effect on the communication system as well.

Synchronization

The unique ID of OpenScape Business users used for the synchonization is the DID number. This number is synchronized with the telephoneNumber field of the AD (Active Directory).

Every change done in the Active Directory of the company is immediately synchronized to OpenScape Business. This means that every new user added to AD will also be added to OpenScape Business and an IP user license will be assigned to that user.

Any change done in AD to already synchronized users is reflected immediately to OpenScape Business users.

If a synchronized user is deleted from AD, the firstName, sn and displayName of the user will be cleared also from OpenScape Business, and the IP user license is released. However, the DID number and internal call number is not deleted from OpenScape Business and remains available to be assigned to another user.

NOTICE: Access to the Active Directory Service is read-only. This means that synchronization of user data is done only from Active Directory to OpenScape Business. Changes in OpenScape Business user info are not synchronized back to Active Directory and will be overwritten by Active Directory data with next synchronization.

Field Mapping

You can customize the mapping of field names to the data schema of the Active Directory Service. In this way, you can control the way fields in OpenScape Business are updated from Active Directory data.

The default mapping of fields is given in the following table:

OpenScape Business field	Active Directory field
first name	firstName
last name	sn
display name	displayName
DID	telephoneNumber

Normalization of DID numbers

The gateway location data of the OpenScape Business system is used to convert the DID number of a user into canonical numnber format.

It is required the format of telephoneNumber in Active Directory to be in canonical format also, so that automatic synchronization is possible.

23.5.1 How to Configure the Active Directory Service

Prerequisites

You are logged into the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Active Directory Integration Service** wizard.
4) Click on the **Active** check box to activate the Active Directory Integration Service.
5) Set the **IP address** of the Active Directory server, the **Username** and **Password** for a valid user.

   The **Username** requested here is not an OpenScape Business user name, but an ActiveDirectory username that must be given in X.500 Directory Specification format. In this format, users are defined with the following nodes:

CN	Common Name
OU	Organizational Unit
DC	Domain Component

   The username is described from the more specific information on the left to the most general on the right. Each piece of information is given in the form of pairs separated with an equal sign (=).

   An example of a username would be `CN=John.doe,OU=Administrators,DC=SomeCompany`.

6) Click on **Fetch DNs** to fetch the available DNs and select one of them as a root base namingContext.

   If there any problem with the user credentials, you will see an error `Authentication error! Please check your credentials.`

7) Edit the **Container** and **Filter** fields, if it is needed.

   The default value for container is `cn=Users` and for filter is `(&(objectCategory=person)(objectClass=user))`

8) Click on **Fetch data**.

   The first 1000 entries of AD will be shown, ordered by lastname(sn).

9) Click on a user to check the details.

10) Click on **OK & Next** to go to the **Field Mapping** screen.

11) Make the neccessary edits in the field mapping values.

    The values on the left column are the OpenScape Business database schema, and the values set on the right column correspond to the Active Directory attributes.

    Telephone Number will be used to match the OpenScape Business DID number.

12) Click on **Finish** to complete the Active Directory Integration

23.6 Application Launcher

Application Launcher is a Java-based Windows application for the call-related control of applications running on the client PCs of UC Suite users and myAgent users. Application Launcher could typically be used to automatically open the contact form in a CRM system for each respective caller, for example.

Application Launcher provides the following features:

- Obtaining call-related information on a phone number (e.g., phone number, name of the caller, customer ID) from either the Open Directory Service or from system directories
- Launching Windows applications or web applications for incoming and outgoing calls
- Transfer of call-related information to Windows applications or web applications
- Automatic operation in the background for incoming calls
- Optional, configurable screen pops for incoming calls with call-related information and buttons for user actions
- Caller list with call function
- Preview functions for testing during configuration
- System configuration profile for simple transfer of the configuration settings of the first configured client to all other clients

23.6.1 Prerequisites for Application Launcher

In order to use Application Launcher, the client PC of the individual user must be equipped with the appropriate hardware and software.

Local administrator rights on the client PC are required for the installation, but not for automatic updates.

Operating System

Application Launcher can be used in combination with the following operating systems:

- Microsoft Windows 10 / 8.1 / 8 / 7 (both 32-bit or 64-bit are possible)
- Microsoft Windows Vista (32 bit)

INFO: The used operating system always requires the latest version of all available updates (Service Packs and patches).

Windows Update

The PCs always need the current status of all available updates, including Service Packs.

Additional Software

Oracle Java 8 or higher or alternatively OpenJDK 8 (see **Service Center** > **Software**)

Web Services for Mobile Phones

Web services for mobile phones has been enabled in the system for the system connection. The ports configured in the system must be open in the firewalls on the LAN and the client PCs.

Open Directory Service (optional)

If Application Launcher is to use the data from the Open Directory Service, the Open Directory Service must be configured in the system. The port configured for this in the system must be open in the firewalls on the LAN and the client PCs.

Related concepts

Configuring myPortal to go and Mobility Entry on page 908
Open Directory Service on page 1120

23.6.2 Profile with Configuration Data for Application Launcher

A profile with configuration data for Application Launcher enables the easy and fast configuration of Application Launcher on all client PCs.

The profile contains all the configuration data, except for the system connection and the user data. As soon as Application Launcher has been fully configured for an initial user, as an administrator, you can make that profile with the Application Launcher configuration data available in the communication system. All other users can then perform the configuration of Application Launcher by importing this profile.

23.6.2.1 How to Provide a Profile with Configuration Data for Application Launcher

Prerequisites

Application Launcher is a fully configured for a user.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click in the navigation tree on **Applications** > **OpenScape Application Launcher**.
3) Click on **Browse** and select the following file: `C:\Documents and Settings\<Windows User Name>\Application Data\Tray_Tool\profile.xml`.
4) Click on **Open**.
5) Click on **Load**.

Next steps

All users can import this profile in Application Launcher and thus perform the configuration.

23.7 myPortal for Teams overview

myPortal for Teams plugin is used to integrate Microsoft Teams application with OpenScape Business.

myPortal for Teams requires new OpenScape Business V3 Mainboard or OpenScape Business S system and it is supported with software release V3R1 FR2 and later releases.

With myPortal for Teams you can:

- Filter and manage your call history.
- View and search contacts.
- Organize contacts in favorite groups.
- Email contacts.
- Select a controlled device (available for MULAP users).
- Start a call.
- Answer, reject or deflect a call.
- Place a call on hold.
- Transfer a call.
- Make a consultation call.
- Alternate between calls.
- Make an attended transfer.

NOTICE: Search for contacts in external directories, such as LDAP, is not available.

NOTICE: VoIP functionality is not supported for myPortal for Teams.

23.7.1 How to configure myPortal for Teams

Prerequisites

- 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

Step by Step

1) Navigate to **Setup > Cloud Services**.
2) Click Edit next to **Microsoft Teams Client-Plugin**.
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) Enter the **Application ID**,

   The Application ID is generated by the administrator of the Microsoft Azure portal.
5) Click **OK & Download**.

   The plugin is downloaded as a zip file. The downloaded file is a customized plugin based on your system configuration.

NOTICE:

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 How to Import Server Certificates (PKCS#12) on page 986.

23.7.2 How to upload myPortal for Teams to Teams store

Prerequisites

You must have administration rights to Microsoft Teams application.

Step by Step

1) Click on **Apps** in the left navigation of the Microsoft Teams application.
2) Click on **Upload a custom app** and select **Upload for my org**.

   Select the file that you have downloaded form WBM and upload it.

Next steps

Once myPortal for Teams plugin is uploaded, it is available for the users to add it in their Microsoft Teams application.

23.8 Unify Phone

It is possible for OpenScape Business users to make phone calls via the Unify Phone client. This functionality is available both from the Unify Phone client and through the device. To do that, you must configure the Unify Phone connectivity with OpenScape Business and add the Unify Phone users.

The available Unify Phone functionality includes:

- Make/answer calls
- Clear/reject calls
- Hold/retrieve calls
- Pull/Push call
- DTMF support
- Swap call (alternate)
- Call forwarding
- Alternative number
- Call routing
- Access to directory and journal
- 3rd party call control using the following onboard UC clients: myPortal @work, myPortal for Desktop, myPortal for Outlook, myAttendant, my Agent and myPortal for Teams.

Besides the features mentioned above, no other features are released, especially feature codes.

NOTICE: 3rd party call control (CTI control) is currently possible only for Unify Phone Desktop client. Control always takes place via the Unify Phone Desktop Client (Web/PWA) and is not intended for the Unify Phone mobile client. It is possible to move a call to the Unify Phone mobile client after accepting the call. Also, 3rd party call control is not intended to be used in conjunction with an active Unify Phone "alternative number" feature.

23.8.1 How to Configure the Unify Phone Connectivity

Prerequisites

You have entered the value **Upstream up to (Kbps)** under **Setup** > **Wizards** > **Basic Installation** > **Basic Installation** > **Upstream of your internet connection**, in order to conduct simultaneous calls. For example, enter '256' for 2 simultaneous calls.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Unify Phone Connectivity**, to configure the basic connectivity settings.
4) Select the **Enable Unify Phone** check-box to activate the Unify Phone connectivity.

5) Under **Unify Phone Domain Credentials**, enter the following details:
   a) Select the **Domain** from the available drop-down list.

      The following options are available:

      - phoneapp.unify.com
      - Custom

      NOTICE: In case Custom is selected, complete the **Custom Domain** field.

   b) Enter the API Key which is generated for your tenant in **Unify Phone API-Key** field.
6) Under **Simultaneous Unify Phone Calls**, select the number of simultaneous Unify Phone calls from the available drop-down list. This number depends on the upstream value previously configured.

   NOTICE: If the call quality deteriorates, the number of simultaneous calls must be reduced.

7) Click **OK & Next**.
8) In the **Unify Phone Location Number** window select which numbering scheme you want to use. This selection affects SIP and WSI numbers format.

   - To use international numbers, enable the **Use International Numbering** checkbox.

     If International numbers are chosen the wizard prompts to configure missing Location Numbers of Unify Phone route, which are going to be used to form the international number. Also, the Unify Phone route parameters for type of number are updated according to the selection.
   - Internal numbers
9) Click **OK & Next**.
10) Click **Execute function** on the pop-up to create a SIP trunk for Unify Phone.
11) Click **OK & Next** followed by **Finish**.

    NOTICE: It is suggested to save the configuration data, by selecting **Data Backup** > **Backup - Immediate** from the main menu.

Next steps

If you want to disable the Unify Phone connectivity, you first need to delete any Unify Phone users as described in How to Remove or Delete Unify Phone Users on page 1141.

NOTICE: It is vital to delete active Unify Phone users prior to e.g. system migrations, to avoid critical discrepancies between the OpenScape Business database and the cloud database.

23.8.2 How to configure the Unify Phone user instance

Prerequisites

Unify Phone Connectivity is configured.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Unify Phone user instance**.
4) Click **OK and Next** and then **Finish**.

23.8.3 How to Manage Unify Phone Users

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Unify Phone user instance**.

   A list with the configured Unify Phone users appears for the specific system.

NOTICE: If there are already registered Unify Phone users you will be prompted to run the Unify Phone Connectivity wizard without changing the configuration.

23.8.3.1 How to Create New Unify Phone Users

Prerequisites

Unify Phone Connectivity is configured.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Unify Phone user instance**.
   The available Unify Phone users are displayed.
4) Click on **Create** next to **Create a New User For Unify Phone**.
5) At the **Unify Phone User Creation** page, do the following:
   a) The **Trunk access code + Unify Phone user call number** is read-only and is generated automatically according to the selected numbering scheme (international or internal).
   b) Enter the **Unify Phone User callno**.
   c) Enter the **Unify Phone User DID**.
   d) Enter the **First Name**.
   e) Enter the **Last Name**.
   f) Enter the Unify Phone user **Email Address**.

6) Click **OK & Next**.
7) Click **Finish**.
   After this process is completed successfully an email is sent to the typed email address, which enables the Unify Phone user to complete the configuration.
8) Repeat steps 4-6 to add more Unify Phone users.

23.8.3.2 How to Add Existing Unify Phone Users

Prerequisites

Unify Phone Connectivity is configured.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Unify Phone user instance**.
   The available Unify Phone users are displayed.
4) Click on **Add** next to **Add Existing User To Unify Phone**.
5) At the **Unify Phone User Allocation** page, the available users are displayed as icons. To add an existing user do the following:
   a) The **Trunk access code + Unify Phone user call number** is read-only and is generated automatically according to the selected numbering scheme (international or internal).
   b) Enter the **Unify Phone User callno**.
   c) Enter the **Unify Phone User DID**.
   d) You can search for a user by **Name** or **E-mail**.
   e) Select a Unify Phone user using the available icons.

      There are three types of icons for Unify Phone users:

      - Green icons: Available users who are active.
      - Grayed out green icons: Non available users who are not active.
      - Grayed out green icon in red frame: Non available users who are not active, already configured with a number in Unify Phone.

      The Unify Phone user **First Name** and **Last Name** fields are filled in automatically.
6) Click **OK & Next**.
7) Repeat steps 4-6 to add more Unify Phone users.

Next steps

Assign licenses to Unify Phone users as described in How to License Subscribers (Standalone) on page 303 or How to License Subscribers (Internetwork) on page 313.

When integrating a Unify Phone user into a team (MULAP), note the following:

- Only one IP or TDM desk phone can be included in the team with the Unify Phone user. The routing function in Unify Phone is used to determine which end device should be used to signal an incoming call.

- The desk phone in the team with Unify Phone can still be controlled by external applications via TAPI, WSI or CSTA. This also applies when Unify Phone is controlled via 3rd party applications.
- Cordless subscribers are not approved in connection with Unify Phone.

23.8.3.3 How to Edit Unify Phone User Details

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Cloud Services**.

3) Click on **Edit** next to the corresponding Unify Phone user.

4) You can edit the following details:

a) The **Trunk access code + Unify Phone user call number** is read-only and is generated automatically according to the selected numbering scheme (international or internal).

b) The **Unify Phone user call number**.

c) The **Unify Phone user DID**.

d) The Unify Phone user **First Name**.

e) The Unify Phone user **Last Name**.

NOTICE: The Selected Unify Phone User field which contains the e-mail address of the user is not editable.

---

5) Click **OK & Next**.

23.8.3.4 How to Remove or Delete Unify Phone Users

There are scenarios where deleting Unify Phone users from your OpenScape Business system is absolutely necessary. For example:

- When migrating from a test lab system to a real/live system.
- When replacing a mainboard from V2 H/W to V3 H/W or due to H/W failures.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Cloud Services**.

3) Click on **Edit** next to **Unify Phone user instance**.

4) Click on **Edit** next to the corresponding Unify Phone user.

5) Click on **Remove** or **Delete**.

6) Repeat steps 1-5 to delete more Unify Phone users.

Keep in mind that deleting admin users is different than deleting non-admin Unify Phone users:

When Unify Phone users, with administrator role or not, are removed from the system, they are not removed from the Unify Phone tenant they belong

to. These users still exist but they do no longer have a phone number assigned to them.

When Unify Phone users without administrator role are deleted from the system, they are also removed from the tenant they belong to.

When Unify Phone users with administrator role are deleted from the system, they are not removed from the tenant they belong to. These users still exist but they do no longer have a phone number assigned to them.

NOTICE: If a new system is set up via cloning or data restore (migration), where the original system had a Unify Phone connector access configured, it must be ensured that any discrepancies between the UP cloud state and that of the OSBiz database will be avoided. For this reason, it is essential to remove any UP users if needed and then disable the Unify Phone connector before cloning/backing up the original system.

23.8.3.5 How to prepare Alternative number and Call routing for Unify Phone interworking

In order for the Alternative number and Call routing functionality of Unify Phone to be supported by OpenScape Business, you need to do the following setting in Expert mode.

Step by Step

1) In **Expert mode**, click **Telephony Server** > **Incoming Calls** > **Call Forwarding**.
2) Click on the **Call dest. list - Definition** tab.
3) Under **Edit Call Forwarding** do the following configurations:
   a) As **Target 1** select `* Called station`.
   b) As **Target 2** select `** User defined`.
   c) As **Target 3** select `Number of Voicemail` (optional).

23.9 Let's Encrypt Service

Let's Encrypt is an automated certificate authority offering free TLS/SSL certificates through the Automatic Certificate Management Environment (ACME) protocol. The service verifies domain ownership using unique tokens and challenges, such as the HTTPS challenge. Upon verification, Let's Encrypt servers provide signed certificates for secure communication between servers and users.

For V2 mainboards systems utilizing OCAB or Booster Server, the Let's Encrypt certificate is synchronized within the Booster server. To facilitate activation, a mechanism is integrated into the Java Application. The activation process of V2 mainboard systems may require additional time as the certificate needs to be transferred and activated within the Booster (either Card or Server). You should anticipate a slight delay in activation time due to this synchronization process.

When the feature is deactivated, the default server certificate is enabled for either the OCAB or Booster Server.

23.9.1 How to configure Let's Encrypt service

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **Let's Encrypt Service**.
4) Under **Domain name configuration**, enter the following details:
   - Type the domain name in the **Primary Domain Name** field.
   - Optionally, type a second domain in the **Secondary Domain Name (Optional)** field.
5) Under **Automatic Certificate Update Configuration**, set the time for the automatic update to take place in the **Automatic Update Time** field.

   NOTICE: Systems restarts upon an automatic update.

6) Click on **Activate** to activate or **Deactivate** to deactivate the service.
7) Under **Let's Encrypt Service Status** you can find detailed information regarding the service and its status:
   - **Service Status** shows whether the service is currently `Active` or `Inactive`.
   - **Certificate Activation Date** shows the date which the certificate was activated.
   - **Renewal date** shows the due date for the automatic certificate renewal.
   - **Renewal Status** shows the status of the automatic renewal process.

   NOTICE: Let's Encrypt protocol uses the HTTP port TCP/80 for the HTTP challenge, during the initial certificate creation or the certificate update.

In WBM home page a message is displayed informing system administrators when the certificate expires (X days), and when the certificate update attempt was unsuccessful.

23.10 CloudLink Service

CloudLink enables communication between on-premise OpenScape Business systems and cloud-based Mitel applications.

SIP Connection

The SIP Connection feature is used to connect OpenScape Business to cloud services like Workflow Studio.

NOTICE: A Workflow Studio license is required.

To enable this feature see chapter How to configure SIP Connector.

INFO: Before doing so, make sure that the upstream of your internet connection is configured (see How to Configure Internet Access via an External Internet Router).

Container support in OpenScape Business

A container runtime is available in OpenScape Business to support the CAS (Cloudlink Gateway) container. Due to performance/capacity constraints it is only available in the following OpenScape Bisness flavors:

- V3 Mainboards with NVMe disk attached (embedded systems)
- OpenScape Business S systems (server variants)

On embedded systems, the container runtime comes preinstalled as part of the OpenScape Business Software Image for V3 HW. It is not started by default on boot in order to save system resources. It is only activated once the administrator enables container support in the Cloudlink Web UI.

On server variants, the container runtime (docker package) must be installed by the administrator when installing the SLES15 operating system.

To configure the container support service see chapter How to configure CloudLink Daemon web interface.

23.10.1 How to configure CloudLink service

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **CloudLink Service**.
4) Click on the checkbox next to **Enable CloudLink Service**.
5) If needed, click on the checkbox next to **Use Proxy**.
6) Type the proxy's IP address and port in the **HTTP-Proxy** and **HTTP-Proxy Port** fields respectively.
7) Click on **Apply** to save your settings.
8) Click on the **CloudLink** button to open the CloudLink Daemon web interface window.

23.10.2 How to open the CloudLink Daemon web interface

CloudLink Daemon web interface allows the configuration and integration of cloud and on-premise systems enhancing the capabilities of OpenScape Business communication applications.

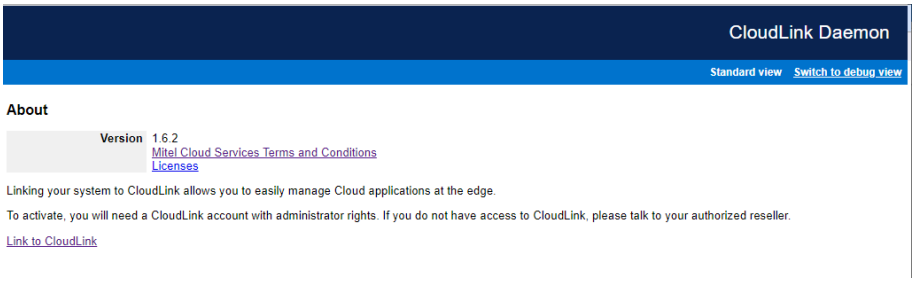
Prerequisites

The upstream of your internet connection is configured (see How to Configure Internet Access via an External Internet Router).

A CloudLink account is required and a connection to CloudLink needs to be established (see How to configure CloudLink service on page 1144).

Step by Step

1) Click on **Link to CloudLink**.



   You will be transferred to the CloudLink Portal.
2) Provide your **username** and **password** to login to the CloudLink Portal.
3) Start a connection.

23.10.3 How to configure CloudLink Daemon web interface

You can perform the following actions using the Standard view or the Debug view. To switch between views click on **Switch to debug view** or **Switch to standard view**.

Step by Step

1) Click on **Mitel Cloud Services Terms and Conditions** to view the terms and conditions.
2) Click on **Licenses** to view related licenses.
3) Click on **Disconnect from CloudLink** to disconnect from the service.
4) Change the day and hour for automatic updates to take place and click on **Reschedule**.
5) Click on **Pause** to pause the next update.
6) Click on **Start all tunnels** and **Stop all tunnels** to start or stop configured tunnels.
7) Click on **Start** or **Stop** to start or stop remote access via CloudLink gateway portal.
8) For V3 mainboards OCCe with NVMe and OpenScape Business S systems, you can configure the container support feature by doing the following:
   a) Click on **Activate container support**.
   b) In the pop-up confirmation window, click **Yes**.
   c) If needed, click **Restart** or **Deactivate container support**, to restart or stop the service respectively.

23.10.4 How to enable / configure SIP Connector to connect to Workflow Studio

Prerequisites

The upstream of your internet connection is configured (see How to Configure Internet Access via an External Internet Router).

A CloudLink account is required and a connection to CloudLink needs to be established (see How to configure CloudLink service on page 1144).

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **CloudLink Service**.
4) Click on the checkbox next to **Enable CloudLink Service**.
5) If needed, click on the checkbox next to **Use Proxy**.
6) Type the proxy's IP address and port in the **HTTP-Proxy** and **HTTP-Proxy Port** fields respectively.
7) Type your credentials in the fields **User name** and **Password**.
8) Click on the checkbox next to **Enable SIP Connector**.
   a) Select a value from the drop-down list for the **Number of Simultaneous CloudLink Calls** field.
9) Click on **OK & Next**.
   The trunks are added (no licenses are needed for the trunks). CloudLink is configured and a connection is established.
10) In the pop-up window you can see connectivity status. Click **Finish**.

23.11 CloudLink Pilot Numbers

Calling any configured CloudLink pilot number routes the call to Wokflow Studio for further processing.

Pilot numbers for the Cloudlink services per OpenScape Business system are going to be limited to 60 per OpenScape Business system.

Trunk lines per OpenScape Business system are limited by the overall trunk lines capacity of 250.

Additionally, trunk lines are limited by upstream bandwidth defined in the basic installation wizard (128Kbps per line).

Cloudlink trunk interconnection is going to occupy 1 of 10 dedicated ITSP/ Native-SIP routes in an OpenScape Business system.

23.11.1 How to configure CloudLink Pilot Numbers

Prerequisites

The CloudLink wizard is configured.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click on **Wizards** > **Cloud Services**.
3) Click on **Edit** next to **CloudLink Pilot Numbers**.
4) Click **Add**.
5) Under **CloudLink Pilot Numbers** column, enter the numbers as needed.
6) For each number enter a name, under **Display Name** column.
7) Click **OK & Next**.
8) If needed, click on **Delete** or **Delete All** to delete a single or all entries, followed by **OK** to confirm the deletion.
9) Click **OK & Next** followed by **Finish**.

24 Accounting

Accounting includes the collection of call data and account codes, the transmission and display of connection data, cost control and accounting tools.

24.1 Connection Data

Connection data includes the collection of call data and account codes.

24.1.1 Connection Data Recording

The system can log the connection data of used lines.

For every completed connection and/or every incoming connection, a connection data record is created. A separate connection data record is stored for each new connection segment (for example, as a result of transferring or forwarding to another subscriber). Internal connections are not logged.

The administrator can enable the following options for recording connection data:

- Recording on or off
- Connection duration
- Currency amounts or call charge units:

  Call charge units are converted into currency amounts based on the configurable call charge factor (currency amount per call charge unit).
- Decimal format

  Divides the currency amount by100 to display 6 cents as 0.06, for example
- Suppress last four digits of destination numbers
- Log incoming connections
- Outgoing calls without connection:

  For example, this gives the calling party proof that the destination station did not accept the attempted call (marked with the connection duration 00:00:00). This option applies to ISDN connections and to all subscribers.
- Connection protocol

  Start logging on beginning the call
- Log MSN
- Output LCR number outgoing or dialed number incoming
  - outgoing:

    the actual call number which is sent by LCR to the PSTN
  - incoming:

    the originally dialed internal number

If call charges accrue before the call is set up (as occurs in Austria, for instance), these are recorded, irrespective of whether or not logging of outgoing calls without connection is enabled.

The system takes connections via QSIG trunks into account only if a trunk code has been configured for them.

No logging occurs for:

- premature termination of the call attempt
- unauthorized connections (LCR, Denied lists).

Related concepts

Account codes on page 1153

24.1.1.1 How to Enable or Disable Connection Data Recording

The **Call Detail Recording** wizard can be used to activate the recording of connection data.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Call Detail Recording** wizard.
4) Select one of the following options:
   - If you want to enable connection data recording, enable the check box **Activate Call Charge Recording**.
   - If you want to disable connection data recording, disable the check box **Activate Call Charge Recording**.
5) Click on **OK & Next** followed by **Finish**.

24.1.1.2 How to Activate or Deactivate Logging of the Connection Duration

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Call Duration**.
   - If you want to deactivate the function, clear the check box **Call Duration**.
5) Click on **Apply** followed by **OK**.

24.1.1.3 How to Configure the Logging of Currency Amounts or Call Charge Units

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want the system to log currency amounts, enable the check box **Display amounts instead of units**.
   - If you want the system to log call charge units, clear the check box **Display amounts instead of units**.
5) Click on **Apply**, followed by **OK**.

24.1.1.4 How to Configure Call Charge Factors, Currency and Computing Accuracy

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Factors**.
4) For each relevant route, enter the appropriate values in the **Multiplier** and **Multi-ISDN** fields.
5) Enter the appropriate value in the **Currency** field at the lower end of the form.
6) For each relevant route with the QSIG protocol, select one of the following options in accordance with the connected communication system:
   - If currency amounts are to be received and sent, select the **Charges** (Currency Amount) check box.
   - If call charge units are to be received and sent, clear the **Charges** (Currency Amount) check box.
7) In each row with a route with the QSIG Protocol which receives and sends call charge units, enter a blank under **Currency**.
8) From the **Computing accuracy** drop-down list, select the entry **No decimal digit**, **1 decimal digit**, **2 decimal digits**, **3 decimal digits** or **Via call charge pulse**.
9) Click on **Apply**, followed by **OK**.

24.1.1.5 How to Activate or Deactivate the Logging of the Last Four Digits

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Last 4 digits suppressed**.
   - If you want to deactivate the function, clear the check box **Last 4 digits suppressed**.
5) Click on **Apply** followed by **OK**.

24.1.1.6 How to Enable or Disable Outgoing Call Logging without a Connection

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Outgoing without connection**.
   - If you want to deactivate the function, clear the check box **Outgoing without connection**.
5) Click on **Apply** followed by **OK**.

24.1.1.7 How to Enable or Disable the Logging of Incoming Calls

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Log incoming calls**.
   - If you want to deactivate the function, clear the check box **Log incoming calls**.
5) Click on **Apply** followed by **OK**.

24.1.1.8 How to Activate or Deactivate the Connection Log

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **On Ringing**.
   - If you want to deactivate the function, clear the check box **On Ringing**.
5) Click on **Apply** followed by **OK**.

24.1.1.9 How to Activate or Deactivate MSN Logging

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Output MSN**.
   - If you want to deactivate the function, clear the check box **Output MSN**.
5) Click on **Apply** followed by **OK**.

24.1.1.10 How to Activate or Deactivate the Decimal Format

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Decimal format**.
   - If you want to deactivate the function, clear the check box **Decimal format**.
5) Click on **Apply** followed by **OK**.

24.1.2 Account codes

Account codes (ACCT) can be used to assign connection data and charges to specific projects. For this purpose, the system logs the account codes entered by users on their phones in the relevant connection data records.

ACCT is used in combination with connection data recording and is available to all subscribers.

The subscriber can enter an ACCT at the phone before or after dialing. It is not possible to dial from a client with ACCT enabled.

An ACCT entered during a conference with external stations is assigned to all participating connections and trunks.

The administrator can set whether an ACCT should be saved for redialing.

The personal directory (also called a phonebook) can save the code for the ACCT feature + an ACCT + a phone number together in one entry:

ACCT Input Procedure

The administrator defines the ACCT input procedure in the LCR dial plan:

- Mandatory

  The ACCT must be entered before setting up the connection (before or after seizing a route).
- Optional

  The ACCT may optionally be entered before setting up the connection. IP phone clients support input during a call, including incoming calls.

ACCT Checking Procedure

The system can check the validity of an ACCT entered for the following types:

- List verification

  Only predefined ACCTs are valid. After a valid ACCT has been entered, the subscriber can immediately continue dialing. The system rejects an invalid ACCT. "Incorrect entry" appears on the display and a negative confirmation tone is output.
- Check number of characters

  All ACCTs that are theoretically possible with the configured number of digits are valid. After a valid ACCT has been entered by the subscriber, he or she can immediately continue dialing.
- No Check

  The validity of the ACCT is not checked. ACCTs with less than 11 digits must be separated from the other digits dialed by the subscriber with “#”. For ISDN phones, this variant always requires a 11-digit account code; otherwise, no dialing occurs.

If the subscriber determines during a connection that the assigned ACCT is not correct, he or she can enter some other ACCT. The system will overwrite the currently set account code. Connection data recording creates a connection data record after each segment. Therefore, previously completed connection segments will be identified with the old account code number.

Related concepts

Connection Data Recording on page 1148

24.1.2.1 How to Configure Account Codes

The **Call Detail Recording** wizard can be configure the recording of call charges.

Prerequisites

You are logged in at the WBM.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Call Detail Recording** wizard.
4) Enter the account codes in the input fields of the **Account codes** area with the method described by the wizard.
5) Click on **OK & Next** followed by **Finish**.

24.1.2.2 How to Configure an Account Code Checking Procedure

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Account Codes**.
4) In the row of the respective account code list in the **Checking procedure** drop-down list, select the desired entry: **No check**, **List check** or **Check number of characters**.
   a) Select the desired value from the **Characters to be checked** drop-down list.
5) Click on **Apply**, followed by **OK**.

24.1.2.3 How to Activate or Deactivate Number Redial with ACCT

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **System Flags**.

4) Select one of the following options:
   - If you want to activate the function, select the check box **No. redial with a/c code**.
   - If you want to deactivate the function, clear the check box **No. redial with a/c code**.
5) Click on **Apply**, followed by **OK**.

24.2 Displaying and Transmitting Connection Data

The display and transmission of connection data includes different ways of displaying connection data on system phones and file transfer methods.

24.2.1 Call-Charge Display with Currency (not for U.S.)

The system can display the currency amount transmitted for the current external connection by the network provider on the display of the telephone.

The network provider must support the transfer of currency amounts with the Advice Of Charge (AOC-D or AOC-S) feature. The system aggregates the amounts of the relevant call charge units.

The currency amount can basically be transferred at the following times:

- on starting the call and possibly during the call (AOC-S)
- during the call (AOC-D)

The administrator can avoid inaccuracies in recording connection data via the "Computing accuracy" parameter. The computing accuracy determines:

- the number of decimal digits for evaluating the connection data (minimum currency amount)
- the maximum total of cumulative currency amounts.

The preset computing accuracy must equal to or higher than the computing accuracy used for ISDN. If the maximum of three decimal places is insufficient, the system automatically rounds up the number to the next unit. Possible values for computing accuracy:

Computing accuracy	Minimum currency amount	Maximum currency amount
No decimal digits	1	around. 4.3 billion
1 decimal digit	0.1	around 430 million
2 decimal digits (e.g., for Euro)	0.01	around 43 million
3 decimal digits (e.g., for British pounds sterling)	0.001	about 4.3 million

24.2.1.1 How to Configure the Call-Charge Display with Currency

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Factors**.
4) For each desired route, from the **Advice of charge** drop-down list, select the entry **Interim**, **Final**, **Interim final** or **No charges**.
5) Select the number of decimal places to be taken into account in the **Computing accuracy** drop-down list at the bottom end of the form.
6) Click on **Apply**, followed by **OK**.

24.2.2 Displaying the Connection Charges on the Phone

The system can display information about the cost of an existing external connection on the phone display as a currency amount.

The system aggregates the amounts of the relevant call charge units. The currency amount is calculated from the call charge units and the configured call charge factor. The service provider must support the Advice Of Charge (AOC) feature.

The connection charges information can be transmitted at the following times:

- On starting the call and possibly during the call (AOC-S)
- During the call (AOC-D)
- At the end of the call (AOC-E)

At the end of the call, the display shows the final charges for the completed call for about 5 seconds, provided the subscriber has not started some other action.

Connection charges for the current connection are always displayed when toggling.

For an unsuccessful blind transfer, the overall amount is displayed and charged.

A subscriber to whom a call is transferred will only see and be charged for the relevant amount from that point in time during the call.

24.2.3 Displaying the Connection Duration on the Phone

The system can show the duration of outgoing and incoming external connections on the phone's display.

The format is HH:MM:SS.

If the connection duration display is disabled, the connection charges information of the PSTN is shown on the phone's display instead. If there is no connection charges information available, the display shows the caller's number (if known).

24.2.3.1 How to Activate or Deactivate the Connection Duration Display

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **Display**.
4) Select one of the following options:
   - If you want to activate the function, select the check box **Call timer display**.
   - If you want to deactivate the function, clear the check box **Call timer display**.
5) Click on **Apply**, followed by **OK**.

24.2.4 Transmission of Connection Data

The system can transmit connection data in a file using HTTPS.

The transmitted file can then be evaluated with a suitable program.

A continuous output of the connection data is only possible via CSTA.

The administrator can choose between the following formats for the connection data (ASCII 8-bit):

- Compressed format
- Uncompressed format

Compressed format, Standard

A connection data record in compressed format contains the following fields, delimited by |, and each connection data record is terminated with CRLF:

Field position	Length	Description
1	8	Date (at end of call)
2	8	Time (at end of call)
3	3	Number of seized trunk
4	16	Internal station number
5	8	Alert time for incoming connection
6	8	Duration of the connection
7	Max. 25	Dialed or received external station number
8	11	Call charge unit/Amount
9	2	Additional information (such as incoming call, outgoing call, transferred connection, conference, DISA, connection setup charges)
10	Max. 11	Acc. code

Field position	Length	Description
11	Max. 11	Only for a point-to-multipoint connection: used MSN
12	6	LCR access code, CO access code
13	2	LCR route used, dial rule
14	25	Dialed or received call number (optional)

Examples of connection data records:

- Outgoing connection:

```
13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||
1||||||
```

- Incoming connection:

```
13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||
1|||||
```

Compressed format, USA-specific

A connection data record in compressed format contains the following fields, delimited by |, and each connection data record is terminated with CRLF:

Field position	Length	Description
1	8	Date (at end of call)
2	8	Time (at end of call)
3	3	Number of seized trunk
4	16	Internal station number
5	8	Alert time for incoming connection
6	8	Duration of the connection
7	Max. 25	Dialed or received external station number
8	11	Call charge unit/Amount
9	2	Additional information (such as incoming call, outgoing call, transferred connection, conference, DISA, connection setup charges)
10	Max. 11	Acc. code
11	Max. 11	Only for a point-to-multipoint connection: used MSN
12	6	LCR access code, CO access code
13	2	LCR route used, dial rule
14	2	PRI Nodal Service
15	1	PRI WATS band
16	3	PRI CIC
17	25	Dialed or received call number (optional)

NOTICE: In *HKEY_LOCAL_MACHINE\SOFTWARE* registry keys for *Accounting Tool*, the value of the **DateFormat DWORD** should be set to 1 for North America date format (MM.DD.YY). The default value is 0 and corresponds to European/Latin America date format (DD.MM.YY).

NOTICE: Data record of Accounting manager in compressed format are seperatrd by the delimiter |. This can be configured only through Manager E.

Uncompressed format

The uncompressed format is suitable for printing. In addition, a header and form feed are output. A connection data record in compressed format contains the following fields, delimited by |:

Field position	Character position, Length	Description
1	1-8 (8)	Date at end of connection: DD.MM.YY (DD = day: value range 01 ... 31, MM = month: value range 01 ... 12, YY = year: value range 00 ... 99)
2	9-16 (8)	Time at the end of a connection segment or an unanswered incoming call: hh:mm:ss a (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59)
3	17-19 (3)	Trunk: trunk number Value range 1 ... 250
4	20-35 (16)	Station: Internal station number For unanswered calls, this is the last station called (e.g., a hunt group, call forwarding, call forwarding—no answer). For group calls, this is the last station entered. For answered calls, the station that accepted the call is shown. A programmed SNO prefix (with networking only) is not output. If the internal numbering was converted to a maximum 7-digit numbering plan, the converted station number is output. The internal station number may be preceded by a max. 7-digit node number If the total resulting from the node number and the station number is greater than seven, only the last seven digits of the number are output.
5	36-40 (5)	Call duration of an incoming connection: mm:ss (mm = minutes: value range 00 - 59, ss= seconds: value range 00 - 59) The display occurs for all incoming calls, provided the output of the ring duration has been configured in the system. If a counter overflow occurs (duration > 59:59), “59:59” is output. A change in date or time during system operation can result in this situation. In the case of an incoming call to a busy station, the ring duration is "00:00".

Field position	Character position, Length	Description
6	41-48 (8)	Duration of the connection or connection segment: hh:mm:ss (hh = hours: value range 00 ... 23, mm = minutes: value range 00 ... 59, ss = seconds: value range 00 ... 59) If a connection has not been established for an incoming call, 8 blanks are output here. If a counter overflow occurs (duration > 23:59:59), “23:59:59” is output.
7	49-73 (25)	Dialed or received external station number (if available): nnnnnnnnnnnnnnnnnnnnnnnnn (n = dialed or received character: value range 0 ... 9, *, #, ?) The output occurs for incoming and outgoing calls, to the extent available. For outgoing calls, the dialed call number or, if available, the call number transmitted via COLP, is displayed. If the data protection function is enabled, the last four digits dialed are replaced by "????" If no station number information is available, 25 blanks are output.
8	74-84 (11)	Call charge units for a connection segment: ddddddddddd (d = digit: value range 0 ... 9) You can select either call charge units or currency amounts. Call charge units are converted into currency amounts using the call charge factor that is defined by the administrator as the currency amount (including any applicable surcharges) per call charge unit. The following applies when setting the call charge factor: • With calculation detail: call charge factor = 100% + any applicable surcharge • Without calculation detail: call charge factor = amount/unit + any applicable surcharge The system records the connection charges with or without a surcharge depending on the calculation detail: The output always occurs whenever connection charges accrue for the connection segment (e.g., even for transferred connections).

Field position	Character position, Length	Description
9	85-86 (2)	Information element: additional information Value range: 0 - 9 Meaning: • 1 = Incoming connection (Voice / 3.1 kHz Audio Call) • 2 = Outgoing connection (Voice / 3.1 kHz Audio Call) • 3 = Incoming connection (Other Services) • 4 = Outgoing connection (Other Services) • 5 = Incoming connection, routed • 6 = Outgoing connection, routed • 7 = int/ext/ext conference with incoming connection / transit through external transfer • 8 = Conference with outgoing connection / Transit through external transfer • 9 = Outgoing connection via call forwarding to external destination • 0 = Connection information (caller list) is output immediately on receiving an incoming call (the output can be suppressed). This can be used, for instance, for a database search from a PC. In cases where multiple stations are called, a separate line is output for each individual station (without ring duration, connection duration, call charge information). • +10 = Offset as a code for blacklisted calls • +20 = Offset as a code for connection setup charges (connection setup without connection duration) • +30 = Offset as a code for a follow-up data record in the case of – Call duration > 24 h. – contiguous connection segments with the same line/station number (e.g., after transferring a connection or clearing a conference). • +40 = Offset for a data record with transit code (by an extension in the subsystem). Can occur in combination with offset +30. • +50 = Offset as a code for DISA connections • +70 = combination of offsets +30 and +40
10	87-97 (11)	Account code (ACCT) entered by the user for this connection: aaaaaaaaaaa (a = ACCT digit: value range 0 ... 9) Missing digits are replaced by spaces.
11	98-108 (11)	Used MSN: mmmmmmmmmmm (m = digit of the MSN: value range 0 ... 9) The output occurs if the user has programmed an MSN key. For outgoing connections of a MULAP subscriber, the call number of the seized MULAP is displayed. Missing digits are replaced by spaces.
12	109-113 (5)	Seizure code used, access code: sssss (s = digit of the seizure code: value range 0 ... 9)

Field position	Character position, Length	Description
13	114-115 (2)	Used LCR route: rr (r = digit of the selected route: value range 0 ... 9)

Communication Sequence

The transfer of connection data can be requested (download request), whereupon the system responds accordingly (download response).

Subsequently, the deletion of connection data can be requested (delete request), whereupon the system responds accordingly (download response).

Download Request - Definition

Element	Contents
HTTP header	Request method = GET
URL	https://<IP address of the system>/management/portlet
Parameters	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username = <username>
	password=<password>

NOTICE: When accessing charge data with the referenced interface, HTTP GET request restrictions are applied. The following special characters are not allowed to be used as pass word, when someone attempts to get data via URL request:

:/?#[]@ !$&'()*+,;=

Example:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Download Response - Definition

Element	Contents
HTTP header	ContentType = "text / plain"
Parameters	attachment filename = "<charging file>"
	data = <content of the charging file>

Response Code	Meaning
SC_OK(200)	Success
SC_BAD_REQUEST(400)	Missing parameter in request
SC_UNAUTHORIZED(401)	Login failure or wrong user name or password
SC_INTERNAL_SERVER_ERROR(500)	Internal error

Delete Request - Definition

Element	Contents
HTTP header	Request method = POST
URL	https://<IP address of the system>/management/portlet
Parameters	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username = <username>
	password=<password>

Example:

```
https://192.148.108.151/management/portlet/?portlet=
hipath-
accountingdownload::HiPathAccountingDownloadPortlet&
entity=accounting&action=delete&username=xbert@system&
password=not4u;-)
```

Delete Response - Definition

Response Code	Meaning
SC_OK(200)	Success
SC_BAD_REQUEST(400)	Missing parameter in request
SC_UNAUTHORIZED(401)	Login failure or wrong user name or password
SC_INTERNAL_SERVER_ERROR(500)	Internal error

Related concepts

Accounting Tools on page 1166

24.2.4.1 How to Select the Format

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options:
   - To select the compressed format, enable the check box **Compressed Output**.
   - To select the uncompressed format, clear the check box **Compressed Output**.
5) Click on **Apply**, followed by **OK**.

24.2.4.2 How to Enable or Disable Transmission of Connection Data via HTTPS

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **Call Charges** > **Call Charges - Output Format**.
4) Select one of the following options in the **Output** drop-down list:
   - If you want to enable the feature, select the item **HTTPS**.
   - If you want to disable the feature, select the item **None**.
5) Click on **Apply**, followed by **OK**.

24.3 Cost control

Cost control includes the features Expensive Connection Route Advisory and Toll Fraud Monitoring.

24.3.1 Expensive Connection Route Advisory

If the telephone is currently unable to reach a call destination via the least-cost routing path, it can notify the subscriber of the use of an expensive connection path via an advisory signal.

The subscriber can thus decide whether or not to conduct the call at that time despite the expensive connection path. The advisory signal may occur as follows:

- Text in the display
- Tone
- Text in the display and tone

The system issues an advisory message for the expensive connection path if a corresponding warning has been configured in the routing table and if the system is not using the route of index 1 of the routing table.

The advisory message is only displayed on the screen if no name is configured for the associated dial rule. If a name is configured, it is displayed.

24.3.1.1 How to Configure an Expensive Connection Route Advisory

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click **Telephony** > **LCR**.
3) Click **Routing** > **LCR** > **Routing table** and then on the appropriate routing table.
4) For every expensive connection route (**Route** column), select the desired entry from the **Warning** drop-down list: **Tone**, **Display** or **Display + Tone**.
5) Click on **Apply**, followed by **OK**.

24.3.2 Toll Fraud Monitoring

The system can monitor connections to detect possible occurrences of toll fraud. Monitoring is performed for connections that arrive via a trunk and then leave via a trunk.

The first station signals when the configured connection duration is exceeded and thus enables you to disconnect the call if required. As an administrator, you can configure whether or after what connection duration such a connection is to be signaled.

24.3.2.1 How to Enable or Disable Toll Fraud Monitoring

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **Time Parameters**.
4) Select one of the following options:
   - If you want to enable Toll Fraud Monitoring, select the desired entry for **Timer for Toll Fraud Monitoring** in the **Base** drop-down list and enter a value other than 255 in the **Factor** field. **Base** * **Factor** is the connection duration after which a potentially fraudulent connection is signaled.
   - To disable Toll Fraud Monitoring, enter the value 255 for **Timer for Toll Fraud Monitoring** in the **Factor** field.

5) Click on **Apply**, followed by **OK**.

24.4 Accounting Tools

Accounting tools are provided by Accounting Manager and Teledata Office.

Related concepts

Service Center – Documents on page 122
Transmission of Connection Data on page 1157

24.4.1 Accounting Manager

Accounting Manager is a Windows application for retrieving connection data via HTTPS and evaluating this data using tables and graphics.

Accounting Manager ships with its own documentation. Accounting Manager retrieves connection data from the individual network nodes. You can also use Accounting Manager to test the Connection Data interface. You can download Accounting Manager in the **Service Center** of the WBM. Accounting Manager requires local administration rights and the activation of TLS 1.2 in Microsoft Internet Explorer.

24.4.2 Teledata Office

Teledata Office is a Windows application for analyzing connection data.

25 Maintenance

The system offers several maintenance options. This includes changing the telephony settings, backing up and restoring the configuration data, updating the software with updates and upgrades and restarting/reloading functions. In addition, appropriate functions for status identification, monitoring and maintenance are available. Remote access to the system is possible via different Remote Services.

Maintaining the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, several maintenance options are offered by UC Booster Server as well. The maintain the UC Booster Server, the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

25.1 Telephony Configuration

The communication system offers various configuration options for telephony, e.g., date and time, SNTP, customized display, and Music on Hold.

25.1.1 Date and Time

The communication system features a system clock with date and time. This system time is shown in myPortal for Desktop and on every terminal's display.

You can define the basic system time or synchronize it as follows:

- via a time server using SNTP
- via an ISDN trunk through an outgoing call
- by a manual setting

System-specific settings are not possible for the system time after activating an SNTP server.

If ever an SNTP server cannot be reached and HFA system phones use a different time source than the system, the time displayed on the phones may differ from the system time.

A system time manually set after system startup is always overwritten by ISDN time information the first time an outgoing ISDN call is made, provided the network provider transmits this information. If the difference between the system time manually set and the ISDN time information in a live system is between 2 and 70 minutes, the ISDN time information is applied. Otherwise, the system time manually set is maintained.

The administrator can select one of the following formats to display the date on the terminal. The format is additionally dependent on the type of phone:

Date format	OpenStage	OptiPoint 410, OptiPoint 420
Europe	Tue 20.11.07	20. NOV 07
USA	Tue 11/20/07	Tue NOV 20.07

Date format	OpenStage	OptiPoint 410, OptiPoint 420
International1	Tue 20.11.07	Tue 20 NOV 07
International2	Tue 20.11.07	TUE 20.11.07

If you inadvertently set a date before 2007 as an administrator, you will subsequently no longer be able to access the WBM. This will only be possible after a restart, which resets the date to 01.01.2007.

25.1.1.1 How to Configure the Date and Time Manually

Prerequisites

You are logged into the WBM with the **Expert** profile.

Perform the following steps if the system does not obtain the date and time via digital trunks or via SNTP.

Step by Step

1) In the navigation bar, click **Expert Mode**.
2) In the navigation area, click **Telephony Server** > **Basic Settings** .
3) Click **Basic Settings** > **Date and Time** > **Date and Time** in the menu tree.
4) Enter the **Date and Time**.
5) Click on **Apply**.
6) Click on **Log Out**.
7) Log into the WBM again.

25.1.1.2 How to Set the Time Zone

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click **Expert Mode**.
2) In the navigation area, click **Telephony Server** > **Basic Settings** .
3) Click **Basic Settings** > **Date and Time** > **Timezone Settings** in the menu tree.
4) Select the **Time Zone** in the drop-down list.
5) Click on **Apply**.
6) Log into the WBM again.

25.1.1.3 How to Configure the Date Format

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click **Expert Mode**.
2) In the navigation area, click **Telephony Server** > **Basic Settings** .
3) In the menu tree, click **Basic Settings** > **System** > **Display**.
4) Select the date format from the **Date format** drop-down list.
5) Click on **Apply**.

25.1.2 SNTP

Over SNTP, you can synchronize the date and time of your systems with NTP time servers on a network-wide basis.

SNTP (Simple Network Time Protocol) is a simplified version of NTP (Network Time Protocol), a standard for synchronizing date and time via packet-based communication networks. Your system needs a connection to an NTP server to synchronize date and time. This connection can occur in your local network or on the Internet. A number of different NTP servers are available on the Internet; you can select one that is located in your time zone. Note the conditions of use for the relevant server and, if necessary, request permission.

25.1.2.1 How to Obtain the Date and Time from an SNTP Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click **Expert Mode**.
2) Click on **Telephony** > **Basic Settings** in the navigation tree.
3) Click **Basic Settings** > **Date and Time** > **SNTP Settings** in the menu tree.
4) Enter the **IP Address / DNS Name of External Time Server**, e.g., `0.de.pool.ntp.org`.
5) Select the item **enabled** in the **Operating State of SNTP Server** drop-down list.
6) In the **Poll Interval for External Time Server** drop-down list, select the desired time interval for retrieving the correct date and time from the SNTP server.
7) Click on **Apply**.
8) Log into the WBM again.

25.1.3 Telephone Logos

System telephones with a display may show the logo as a background of the Telephony User Interface (TUI).

As an administrator, you can import, assign or delete phone logos for system telephones with a display. Different types of system telephones may use different phone logos.

Related concepts

Updating System Telephones on page 1196

25.1.3.1 How to Load a Phone Logo into the System

Prerequisites

You are logged into the WBM with the **Expert** profile.

The image file with the phone logo meets the following prerequisites::

Phone	Format	Color
OpenStage 40	112 x 32, BMP	monochrome
OpenStage 60 OpenStage 80	240 x 71, JPEG	monochrome or color
OpenScape Desk Phone CP 400 OpenScape Desk Phone CP 400T/405T	112 x 32, BMP	monochrome
OpenScape Desk Phone CP 600/700/700X OpenScape Desk Phone CP 710	220 x 70, PNG	24-bit with alpha (transparency)
OpenScape Desk Phone CP 600E	220 x 70, PNG	24-bit with alpha (transparency) or 256 greyscale with alpha

You have access to the image file with the phone logo in the file system of the administration PC.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click on **Phone Image Logos** > **Load** in the menu tree.
4) Click **Browse** to select an appropriate image file.
5) Click **Load**.

25.1.3.2 How to Deploy a Phone Logo to System Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click on **Phone Image Logos** > **Deploy** in the menu tree.

4) Select the check box **Deploy** in the row of the phone logo to be deployed.
5) Select the desired system telephone type in the **Deploy to Workpoints with Selected Device Type** drop-down list.
6) Click on **Apply**.

25.1.3.3 How to Delete a Phone Logo

Prerequisites

You are logged into the WBM with the **Expert** profile.

You have access to the image file with the phone logo in the file system of the administration PC.

To delete a phone logo from the communication system, perform the following steps:

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click on **Phone Image Logos** > **Load** in the menu tree.
4) Select the check box **Delete** in the row of the phone logo to be deleted.
5) If you want to delete more phone logos, repeat the previous step.
6) Click on **Delete**. All marked phone logos will be deleted from the communication system.

25.1.4 Customized Display

A customized display enables the company name, for example, to be displayed on system phones in the idle state.

Only the right portion (max. 18 characters) of the second display line, which displays "OpenScape" by default, can be changed. The text lines up with the left part of the date if the length of the text allows it:

```
16:30       FR 29.FEB 08         123456  Post Office Hotel>
```

25.1.4.1 How to Change the Customer-Specific Display (System Name)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Click **Basic Settings** > **Gateway** in the menu tree.

4) Enter the name to be displayed in the **System Name** field.

NOTICE: Do not use any characters other than A-Z, a-z and 0-9.

5) Click on **Apply** followed by **OK**.

25.1.5 Multilingual Text Output

The language for display messages can be selected system-wide or for a specific station only.

Available languages: Bulgarian, Catalan, Chinese, Czech, Danish, Dutch, English (UK), English (US), Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Macedonian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Serbo-Croatian, Slovak, Slovenian, Spanish, Swedish, German (Telekom), Turkish.

You set the language when you enter the country initialization code during system booting.

Related concepts

Configuring Stations on page 429

Related tasks

How to Configure IP and SIP Stations on page 190

25.1.6 Flexible Menus

Flexible menus allow you to customize the menu items shown on the display of system telephones.

As an administrator, you can select the menu items to be shown or hidden individually.

25.1.6.1 How to Edit the Flexible Menu

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) In the menu tree, click **Basic Settings** > **System** > **Flexible menu**.
4) Edit the **Masking list** as follows:
   - To hide a menu item, enable its check box.
   - To show a menu item, enable its check box.
5) Click on **Apply** followed by **OK**.

25.1.7 Music on Hold

The communication system can play back Music on Hold (MOH) to waiting subscribers during switching operations. Callers hear MOH while in the hold state, parked state or transfer state. This also applies to callers in the call distribution queue.

The system can import Music On Hold from the following sources:

- Music On Hold
- EXMR

  See Installing OpenScape Business X1/X1W, Service Documentation or Installing OpenScape Business X3/X5/X8, Service Documentation.
- MUSIC plugin module

  See Installing OpenScape Business X1/X1W, Service Documentation or Installing OpenScape Business X3/X5/X8, Service Documentation.
- MPPI USB EXM module (only for OpenScape Business X3/X5)

  See Installing OpenScape Business X3/X5/X8, Service Documentation.

Audio Files

The administrator can transfer audio files for the internal Music on Hold from the PC to the communication system for use as an alternative internal Music on Hold.

NOTICE: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

IMPORTANT: If the station on hold is an IP workpoint client or an IP trunk, the internal MOH is used. External MOH is not intended for IP.

The audio files must be available as `Wave` files with the following properties:

- 16 bit PCM
- Mono or stereo
- Possible sample rates: 8 / 22.05 / 24 / 32 / 40 / 44.1 or 48 kHz.
- Maximum length for the audio file name: 30 characters

Recommended: **16 bit PCM - Mono - 8 kHz, length approx 2 min**

Music On Hold

Different Music on Hold can be configured for the day and night service.

NOTICE: For UC Suite there is no distinction between day and night files. The **MoH Day File** is used.

The administrator can configure the following functions:

- Music on hold with ringing tone (ringback):

  The subscriber on hold first hears the MOH melody during the consultation. After the party on hold is transferred to the destination, the ring tone is heard instead of the music on hold.
- Music on hold without ringing tone (ringback):

  The held party will hear MOH until the called party answers the call.
- No music on hold:

  The held party hears nothing (silence). The caller hears the ringback tone in the event of an unscreened transfer for an external call.

25.1.7.1 How to Import Internal Music On Hold

The **Music on Hold / Announcements** wizard can be used to import audio files as internal Music on Hold in the communication system.

Prerequisites

You are logged in at the WBM.

The audio files to be imported are available as WAVE files in the required format.

NOTICE: Before using announcements or music, make sure that you do not infringe on any copyrights.

NOTICE: For UC Suite there is no distinction between day and night files. The **MoH Day File** is used.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click on **Wizards** > **Central Telephony**.
3) Click **Edit** to start the **Music on Hold / Announcements** wizard.
4) Go to **MoH Day File** for the day service or **MoH Night File** for the night service and click on **Browse**.
5) Select an audio file and click **Open**. The path to the audio file is displayed at **MoH Day File** and/or **MoH Night File**.
6) Click on **Load**.
7) Confirm the message with **OK** and click **OK & Next**.
8) Click **Finish**.

25.1.7.2 How to Configure the Music on Hold Functionality

Prerequisites

You are logged into the WBM with the **Expert** profile.

The maximum length for the Music on Hold file name is 30 characters.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Auxiliary Equipment** in the navigation tree.
3) Click on **Auxiliary Equipment** > **Announcements / Music On Hold** in the menu tree.
4) In the **Music On Hold** area under the **Type of MOH** drop-down list, select the item **No Music On Hold**, **MOH without ringing tone** or **MOH with ringing tone**.
5) Click on **Apply**, followed by **OK**.

25.1.7.3 How to Change the Music on Hold Functionality for Each CON Group

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony> Auxiliary Equipment** in the navigation tree.
3) Click on **Auxiliary Equipment > Announcements / Music on Hold** in the menu tree.
4) Click on the **Edit Music On Hold** tab.
5) Select the desired music on hold from the Audio File drop-down list in the relevant row of the traffic restriction group.
6) If a CON group does not have any music on hold assigned to it, the internal music on hold is used for the group
7) Enter a Description in the row of the corresponding traffic restriction group.
8) Click **Apply**.
9) Click **OK**.

NOTICE: This functionality is applicable only to OpenScape Buisness S systems and is not supported in OpenScape Business X.

25.1.8 Announcements

The communication system allows on-hold announcements to be played for callers before answering a call and also when using call distribution and DTMF direct inward dialing. You can also replace the MOH melody in certain situations by an announcement, for example, if a party is placed on hold or if a subscriber is busy or being routed.

The system can import announcements from the following sources:

- Internal announcements
- Announcement Player (only with UC Booster functionality)

  The announcement player is an internal software program that is available together with the UC Booster functionality (UC Booster Card or UC Booster Server). On calling a subscriber, the announcement player first plays the desired announcement and then sets up the connection to the subscriber.

- Analog Announcement Device

  See the section on Auxiliary Equipment - Analog Announcement Device in the *OpenScape Business, Administrator Documentation*.
- MPPI USB EXM module (only for OpenScape Business X3/X5)

  For more information, see *Installing OpenScape Business X3/X5/X8, Service Documentation*.

The administrator can configure announcements for single (start/stop) or continuous playback.

An external announcement device must behave like a station, i.e., announce itself, play the announcement and switch the call (enter consultation hold, dial and hang up).

Audio Files

The administrator can transfer audio files with announcements from the PC to the communication system.

NOTICE: Before using announcements or music from other sources, make sure that you do not infringe on any copyrights.

The audio files must be available as `Wave` files with the following properties:

- 16 bit PCM
- Mono or stereo
- Possible sample rates: 8 / 22.05 / 24 / 32 / 40 / 44.1 or 48 kHz
- Maximum length for the audio file name: 30 characters

Recommended: **16 bit PCM - Mono - 8 kHz, length approx 2 min**

25.1.8.1 How to Configure Announcements (UC Suite & UC Booster)

The **Music on Hold / Announcements** wizard can be used to configure the announcements.

Prerequisites

- In **Expert Mode > Middleware > Announcement Player** select the check box **Service will be started automatically** to enable announcement player.
- An announcement player call number should be set in **Expert Mode > Basic Settings > Voicemail / Announcement Player**.
- Verify the number is correctly configured in **Expert Mode > LCR > Dial Plan**, under the **Ann-Player** field.
- The associated **Routing Table** is set to **12**, **UC Suite** is set for **Route** and **MEB** is set for **Dial Rule**.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Central Telephony**.

3) Click on **Edit** to start the **Music on Hold / Announcements** wizard.

4) Skip the selection of **Load Music on Hold Files via HTTP** files, by clicking on **OK & Next**.

NOTICE: Before using announcements or music, make sure that you do not infringe on any copyrights.

---

5) To transfer an audio file to the communication system, proceed as follows:
   a) Click on **Choose File**.
   b) Select an audio file.
   c) Click on **Open**.
   d) Click on **Load**.
   e) Confirm the message with **OK**.
   f) If you want to load more audio files to the system, repeat these steps.
6) Click on **OK & Next**.

INFO: The configuration parameters for **Announcements** are also described and can be configured via **Expert Mode > Auxiliary Equipment > Announcements**.

---

7) Select the type of the announcement to be played in the **Type** column.
8) Select the port to which the device is connected in the **Access** column. External destinations can be used to address announcement devices in another system node.
9) Select an announcement file from the drop-down list in the **Wave File** column (only for **Announcement Player** type and in UC Suite mode).
10) Select the type of playback from the drop-down list in the **Mode** column.
11) Click on **OK & Next**, followed by **Finish**.

25.1.8.2 How to Configure Announcements (UC Smart)

The **Music on Hold / Announcements** wizard can be used to configure the announcements.

Prerequisites

Analog ports that are set up as announcement ports must be assigned the value **Answering Machine** under **Extension Type**.

EVM ports that are set up as announcement ports should be:

- assigned the value **Standard** under **Extension Type**.
- removed from the hunt group of the voicemail box.
- assigned a voicemail box to the call number of the port in Expert Mode**Expert Mode > Auxiliary Equipment > Smart VM**.

Step by Step

1) In the navigation bar, click on **Setup**.
2) In the navigation tree, click **Wizards** > **Central Telephony**.
3) Click on **Edit** to start the **Music on Hold / Announcements** wizard.

4) Skip the selection of **Load Music on Hold Files via HTTP** files, by clicking on **OK & Next**.

INFO: The configuration parameters for **Announcements** are described and can be configured via Expert Mode > Auxiliary Equipment > Announcements.

---

5) Select the type of the announcement to be played in the **Type** column.
6) Select the port to which the device is connected in the **Access** column. External destinations can be used to address announcement devices in another system node.
7) Select an announcement file from the drop-down list in the **Wave File** column (only for **Announcement Player** type and in UC Suite mode).
8) Select the type of playback from the drop-down list in the **Mode** column.
9) Click on **OK & Next**, followed by **Finish**.

25.1.9 User to User Signaling

The communication system enables the transparent transmission of messages between stations (user to user signaling, UUS). UUS1 is supported for information exchange in control messages for connection setup and cleardown.

In the case of a point-to-multipoint connection, it is important to ensure that only one device transmits a message to an incoming call.

25.1.10 Voice Channel Signaling Security

The communication system offers a security mechanism that can be set up by the administrator to prevent undesirable tone injections into the voice channel. No override is possible for a connection protected by this method. Every station configured as a Fax device automatically has this signaling security mechanism.

Recalls are deferred until the extension is free again.

Stations on-hold always have signaling security.

25.1.11 Time Parameters

The communication system offers the administrator options for setting various time parameters such as the "length of callback" or the "timer for automatic redial".

The time parameters are preset in the communication system and should normally not be changed.

25.1.12 Controlling Centrex Features

To control Centrex features, the dial tones for * and # must be transmitted to the ISDN and ITSP.

As an administrator, you can activate or deactivate this feature.

The input of a code must occur in the dialing state (e.g., after entering the trunk code). The input always begins with * or #, followed by a digit or digit combination, and ends with #.

25.1.12.1 How to Enable or Disable the Control of Centrex Features

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Telephony** > **Basic Settings** in the navigation tree.
3) Navigate in the menu tree to **System** > **System Flags**.
4) Select one of the following options:
   - If you want to enable the control of Centrex features, select the check box **Transparent dialing of * and # on trunk interfaces**.
   - If you want to disable the control of Centrex features, clear the check box **Transparent dialing of * and # on trunk interfaces**.
5) Click on **Apply** followed by **OK**.

25.2 Backup and Restore

The communication system's configuration data can be backed up and restored.

The configuration data is saved in a backup set. Every backup creates a separate backup set. Backups can be created manually immediately or scheduled for automatic execution at specific times.

NOTICE: It is strongly recommended to regularly back up the configuration data as backup sets. When updating to a new minor release, it is necessary to create a new backup set. Every backup is encrypted using a system specific key. An encrypted backup set can only be used for the restore of the system that has encrypted the backup.

NOTICE: When performing a data restore for OpenScape Business systems using Unify Phone, please note that it is not possible to reactivate the Unify Phone service / cloud connection or reactivate Unify Phone users via data restore. This is due synchronization issues with the Unify Phone cloud. When performing data restore make sure that Unify Phone service / cloud connection is activated and configured Unify Phone users are the same as in the backup set.

Different backup media can be used to store the backup sets (such as USB media, network drives or the hard disk of the UC Booster Card, for example).

Depending on the system configuration, the use of the communication system and the type of backup medium involved, a backup or restore may take a long

time - in some cases for systems with the UC Suite, up to three hours. This process should not be terminated manually or by a system reboot.

Aborting a data recovery may lead to an inconsistent system configuration in which an error-free operation of the system is not guaranteed. An aborted recovery should always be repeated until it is completed successfully. Otherwise, a complete reconfiguration of the system may be necessary. If the recovery fails repeatedly, please contact the Service Support and make sure in the meantime that your backup is not overwritten by new backups. To do this, the automatic data backup must be temporarily disabled.

Backup Sets for Diagnostic Purposes

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example. Diagnostics backup sets include, among other things, the configuration data of the communication system and the installed UC solution. Voicemails, fax messages and announcements are not included.

"Hard Disk" Backup Directory (Only for UC Booster Card)

If a UC Booster Card is installed, the configuration data of the communication system can be saved in a separate partition on the hard disk of the UC Booster Card in the backup directory. This backup directory is already provided as the standard archive "Hard Disk".

Backing up the Configuration Data of the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, then the configuration data of the UC Booster Server must also be backed up when backing up the configuration data of the system. Backing up the data of the UC Booster Server is basically identical to backing up the data of the communication system; the only difference is that the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

25.2.1 Backup Sets

The configuration data of the communication system is saved in a backup set.

In addition to backup set, a text file associated with the backup set must also be saved. It contains information about the date and time of the backup and under which software version the backup was performed. The text file is necessary for the recovery of the backup set.

If the number of backup sets saved exceeds the set value, the oldest backup sets are deleted.

Backup Set Data

The following data for a backup set is presented:

- **Archive name**: Name of the backup set
- **Size**: Size of the backup set in bytes
- **Date**: Date on which the backup set was created.

- **Comment**: Comment that was specified when creating the backup set (optional).

Backup sets that have been grayed out cannot be restored.

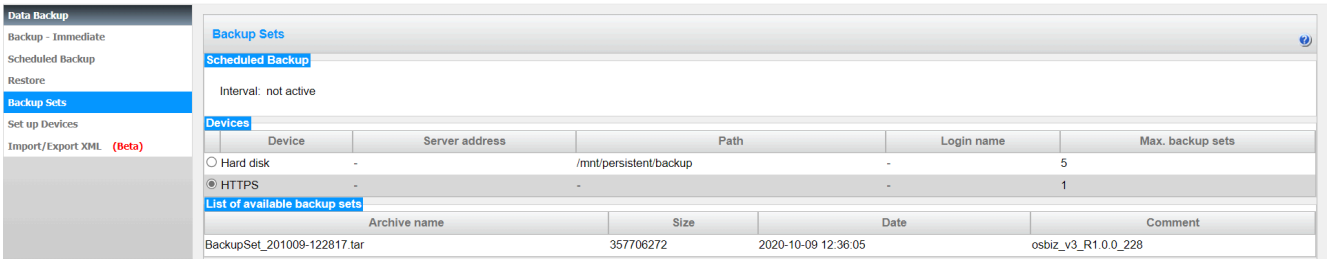
25.2.1.1 How to Display Backup Sets

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) Click **Backup Sets** in the navigation tree.
3) Activate the backup medium containing the backup set you want to have displayed in the **Devices** area. A list of all backup sets available on this medium appears.



25.2.1.2 How to Delete Backup Sets

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Backup and Restore** in the navigation bar.
2) Click **Backup Sets** in the navigation tree.
3) Activate the backup medium containing the backup set you want to have displayed in the **Devices** area. A list of all backup sets available on this medium appears.
4) Select the check box of the backup set you want to delete and click **Delete**. The backup set is deleted.

25.2.2 Backup Media

The backup sets are stored on the selected backup media.

The following backup media can be used for the backup:

- Inserted USB storage device
- Network drive
- Client PC using HTTP (only possible with immediate backup)

- Hard disk of the UC Booster Card
- FTP/FTPS servers

For every backup medium, the maximum number of backup sets to be stored in the directory can be specified.

USB Storage Device

To use a USB storage device (e.g., a USB hard disk or flash drive) for backup, the USB device must be plugged into the USB server port of the communication system. In addition, the USB device must be formatted with FAT-32. Due to filesystem limitation, the maximum size of the backup set cannot exceed 4 GB. In such cases, alternate backup media must be selected. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup!

A bootable USB device is not supported.

With OpenScape Business S and OpenScape UC Booster Server, the USB device is plugged into the USB port of the Linux server.

FTP/FTPS servers and network drives

FTP/FTPS servers and network drives can be added, edited or deleted as new media. FTP/FTPS servers and network drives may also be specified more than once if different directories on them are used. TLS 1.2 is supported as the encrypted file transfer protocol (FTPS).

In order to back up the configuration data, the user must have write permission for the root directory of an FTP/FTPS server. To back up to a network drive, users only need write permission for the desired directory.

If the transmission speed to the FTPS server is too low, there may be a malfunction in the backup. If this occurs, the backup must be restarted.

For FTPS, certificates up to 2048 bits are supported. These certificates are required for authentication at the FTPS server.

25.2.2.1 How to Add a Backup Medium

Prerequisites

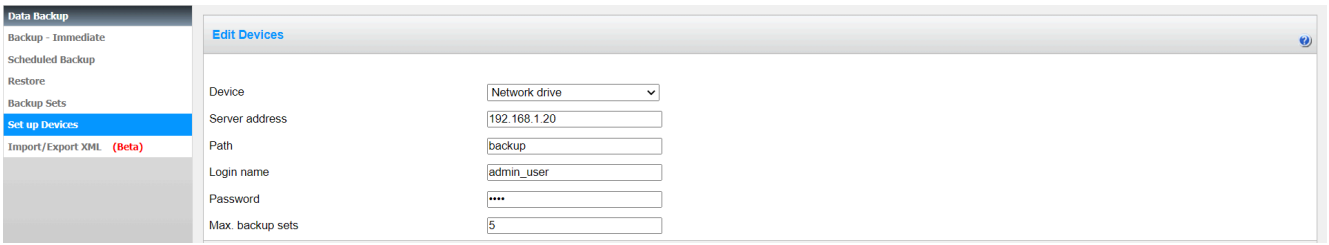
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.

2) Click **Set up Devices** in the navigation tree.

3) Click on **Add**.



4) Select the desired backup medium from the drop-down list in the **Device** column.
   - If you want to save to an FTP/FTPS server, select **(S)FTP**.
   - If you want to save to a network drive, select **Network drive**.

   NOTICE: The supported Samba version is SMB2.

5) Enter the host name or the IP address of the medium under **Server Address**.
6) Enter the path in which the backup set is to be stored under **Directory**.
7) If you want to save to an FTP/FTPS server, enter the **User name** and **Password** for accessing the FTP/FTPS server.

   NOTICE: The accepted characters for the password field are: `0-9 A-Z a-z ~ ! @ # $ % ^ _ - + = ? / , . :`

   The maximum allowed password length is 64 characters.

8) If you want to save to a network drive, enter the **Login Name** and **Password** for accessing the network drive.

   NOTICE: By default, an empty domain is used for authentication. In case you want to provide the domain then use a forward slash (/) character as separator in the **Login name** field. For example: `domain/user`.

9) Under **max. Backup Sets**, enter the maximum number of backup sets that are to be stored in the directory.
10) Click on **OK & Next**. The new backup medium created appears in the list of available backup media.
11) Click **Backup Sets** in the navigation tree.
12) Activate the backup media you just added in the **Devices** area. If no red bar with an error message appears in the list of available backup sets, the backup medium is set up correctly.
13) If an error message is displayed, check your entries again (see How to Edit a Backup Medium on page 1183

25.2.2.2 How to Edit a Backup Medium

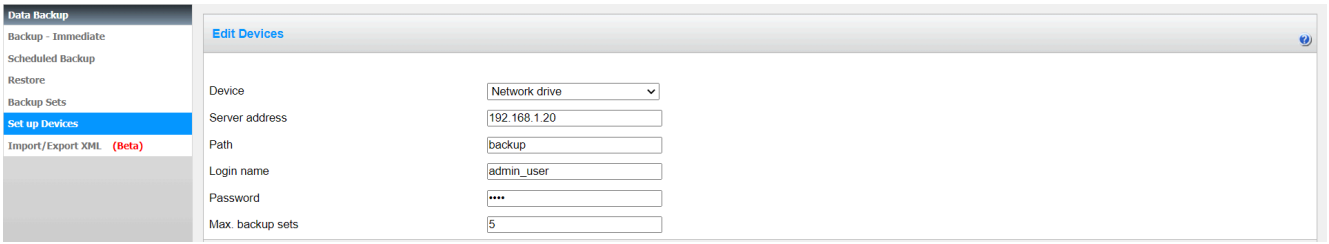
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) Click **Set up Devices** in the navigation tree.

3) Activate the backup medium to be edited and click **Edit**.



4) Change the required values.
5) Click on **OK & Next**.

25.2.2.3 How to Delete a Backup Medium

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) Click **Set up Devices** in the navigation tree.
3) Select the backup medium to be deleted and click **Delete**.

   It is also possible to select multiple backup media for deletion.
4) Confirm the prompt with **OK**. The backup medium is deleted from the list of available backup media.

25.2.3 Immediate Backup

The configuration data can be immediately backed up manually.

A variety of backup media can be used for data backup; By default, the backup medium is set up as **HTTPS**. You can thus store the backup set in all storage locations that can be accessed on the client PC with which you logged into the WBM. The chosen storage location must also be accessible when restoring the backup set. If a USB device is connected to the communication system, **USB Device** is displayed as an additional backup medium. If the UC Booster Card (incl. hard disk) is connected, a further backup medium called **Local hard disk** is displayed.

The name of the backup set is assigned automatically during the backup. It includes, among other things, the date on which the backup was performed. In addition, this data is also included in a text file that must also be stored. If desired, a comment can be optionally added to identify a backup set more easily prior to a subsequent restore.

Related concepts

Scheduled Backup on page 1186

Related tasks

How to Change your Own Administrator Password on page 116

25.2.3.1 How to Save a Backup Set Immediately

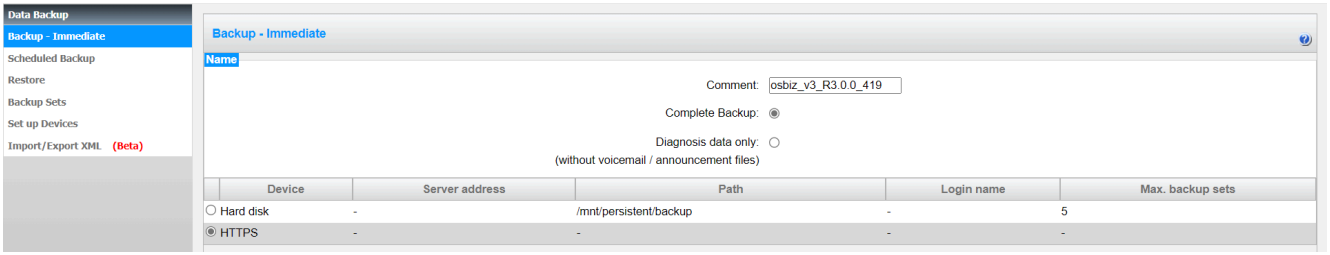
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Only when using UC Suite: UC Suite has started correctly.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) In the navigation tree, click **Backup - Immediate**.



3) Enter a comment for the backup set in the **Comment** field so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) If you want to create a backup set including voice messages and announcements, select the **Full Backup** option.
5) If you want to create a backup set without voice messages and announcements, select the **Only Diagnostics Data** option.
6) Activate the target drive on which the backup set is to be saved in the **Devices** area.
7) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.

NOTICE: If the **OK & Next** button is grayed out, then one or more applications (e.g., UC Suite) for which the data is to be saved were not started correctly.

If you do not have access rights for the selected archive directory, you will receive an error message. Select another destination drive or change the path for the archive.

An error message appears if there is not enough disk space on the destination drive for the backup set. If this occurs, select another destination drive or delete a backup set and restart the backup.

---

8) The backup was successful if the message **Backup completed successfully! 100%** appears.
9) If you have selected **HTTPS** as a backup medium, you must save the backup set and the text file associated with the backup to a location of your choice. This is done automatically for the other backup media. The browser

window must remain open until the save operation for the backup set and text file has been completed.

NOTICE: If you are using a USB device as a backup medium, wait till the LED of the USB device stops flashing. It is only then that the backup has been successfully stored on the USB device. You can then remove the USB device.

10) Click on **Finish**.

25.2.4 Scheduled Backup

You can use a schedule to automatically back up configuration data. The time, frequency and location of the automatic backup is configurable.

The scheduled data backup can be scheduled for a fixed time daily or weekly and then started automatically. This "backup job" can be created for an internal or external backup medium. It is not possible to configure multiple backup jobs.

Related concepts

Immediate Backup on page 1184

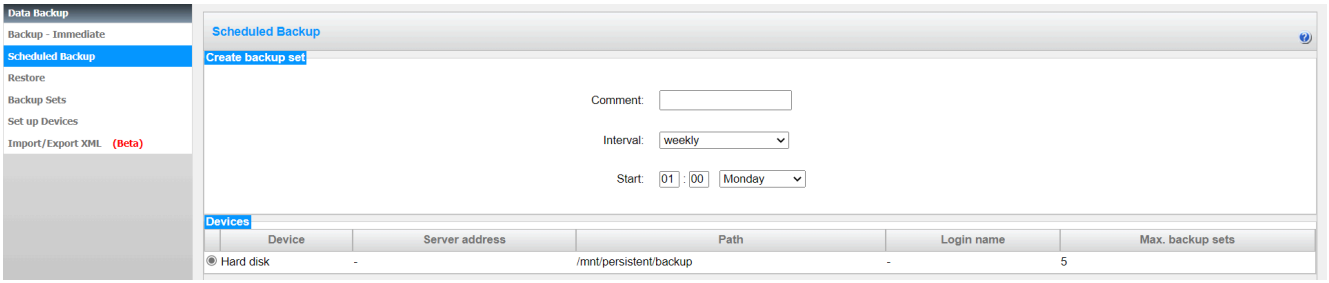
25.2.4.1 How to Save a Backup Set with a Scheduled Backup

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) In the navigation tree, click **Scheduled Backup**.



3) Enter a comment for the backup set in the **Create backup set** area in the **Comment** field so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) Specify the interval for the backup:
   - Daily backup: In the **Interval** drop-down list, select the item **Daily** and then enter when the backup is to be started every day under **Backup on**.
   - Weekly backup: In the **Interval** drop-down list, select the item **Weekly** and then enter on which weekday and at what time the backup is to be started under **Backup on**.

5) Activate the target drive on which the backup set is to be saved in the **Devices** area.
6) Click on **OK & Next**. The backup is started automatically every day (daily) or every week (weekly) at the specified time.

25.2.5 Restore

The restoration of configuration data must be performed manually using the backup sets.

All the supported backup media can be used to restore data;

25.2.5.1 How to Restore a Backup Set

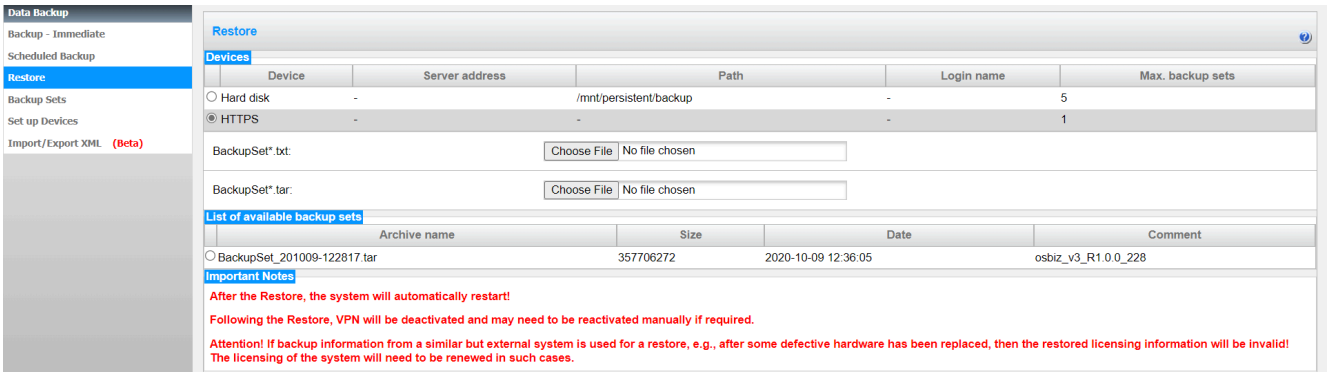
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Only when using UC Suite: UC Suite has started correctly.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) Click **Restore** in the navigation tree.



3) Activate the medium containing the backup set to be restored in the **Devices** area.
4) If you activated **HTTPS** as the backup medium, navigate to the storage location of the backup set and select the backup set. Then navigate to the storage location of the text file and select it.
5) If you activated any other backup medium than **HTTPS**, select the backup set containing the configuration data to be restored in the **List of available backup sets** area.
6) Wait until the files have been loaded onto the system and then click **OK & Next**. The recovery of the configuration data is started. The progress of the restore process is displayed.
7) After the message **Restore complete!** appears, the system will automatically reboot. The restoration is completed successfully when the system is ready for use again.

25.3 Updates

Updates provide the latest software available for the system components within a version.

To install updates, you will need the 3-year software support.

The version of the installed software and the expiration date of the software support are displayed on the home page of the WBM. If more recent software updates are available, this is indicated there.

NOTICE: When updating to a new minor release, it is necessary to create a new backup set.

The software update is performed using the WBM. On a hardware model, the software can also be optionally updated directly from a USB device without WBM access. In a communication system with the UC Booster Server, the hardware model and the UC Booster Server are updated separately.

Using the WBM, the software can be updated via the Internet web server, a local web server or directly via image files.

The following system components are updated:

- Software of the communication system
- Software of the UC clients
- Software for system telephones (updates can also be performed individually)
- Documentation

The software for the UC clients is updated together with the software of the communication system. If a more recent software version is available, users of the UC clients are notified via an Auto-Update message that an update is available and can be installed.

The software update of the IP system telephones occurs automatically with the update of the communication system, but can also be done manually. For UP0 system telephones, the update is performed manually using Manager E.

The software update can be optionally started immediately or by defining the times for the software transfer and software activation independently. The update should be performed outside the business hours of the customer, since the communication system and/or the system telephones are restarted, existing calls are dropped, and the use of the UC clients is interrupted temporarily.

After the software has been transferred to the communication system, it is activated at the selected time. The latest phone image is then automatically loaded onto the IP system telephones. After a restart of the communication system and the IP system telephones, the newly loaded software will be active.

NOTICE: Software update must not performed simultaneously in all systems and in different software versions.

Image Files

To update system components, compressed image files containing the software of the system components are required. These image files can be downloaded from the software server (Internet web server) and stored independently on a

local web server or in the internal network or on a USB stick, for example. There is a separate image file for the communication system without a UC Booster Card and a separate image file for a system with a UC Booster Card. Both image files also include the software for the system telephones. In addition, there is also a separate image file for each type of system telephone type in case the system telephones need to be updated separately.

The following types of image files are available:

- **tgz**: for the software of the communication system. The tgz file contains a tar file. The tar file must be unpacked from the tgz file with a decompressor such as WinZip or 7-zip, for example. The tgz file is offered for download because a check can be performed to determine whether or not the file is corrupted when downloading the software from the server.
- **tar**: for the software of the communication system. It contains the packed files for each system component.
- **app**: for the software of the system telephone.

Local Web Server

When performing a software update via a web server, the software server (Internet web server) is accessed by default.

However, it is also possible to use a local web server for updates. To do this, the image file must be stored on the local web server, and the path to the local web server must be configured in the WBM.

Speed Upgrade

A speed upgrade as with the HiPath 3000 is not possible.

IMPORTANT: Pulling out the SDHC card during operation will result in the loss of data!

Network - Licensing

When upgrading - migrating systems in a network, where the master node is used for licensing the slave nodes, please start with the slave nodes first before the master node.

25.3.1 Using a Local Web Server

The software can be updated via a local web server.

The current image files must be stored on the local web server. In addition, the access data for the local web server must be entered in the WBM. This change can only be performed by an administrator with the **Expert** profile. After the access data of the local web server has been entered, this will be set as the default for all future updates of the communication system. In other words, the local web server will now be used instead of the Internet web server.

25.3.1.1 How to Configure Access to the Local Web Server

Prerequisites

You are logged into the WBM with the **Expert** profile.

A connection to the local web server is available.

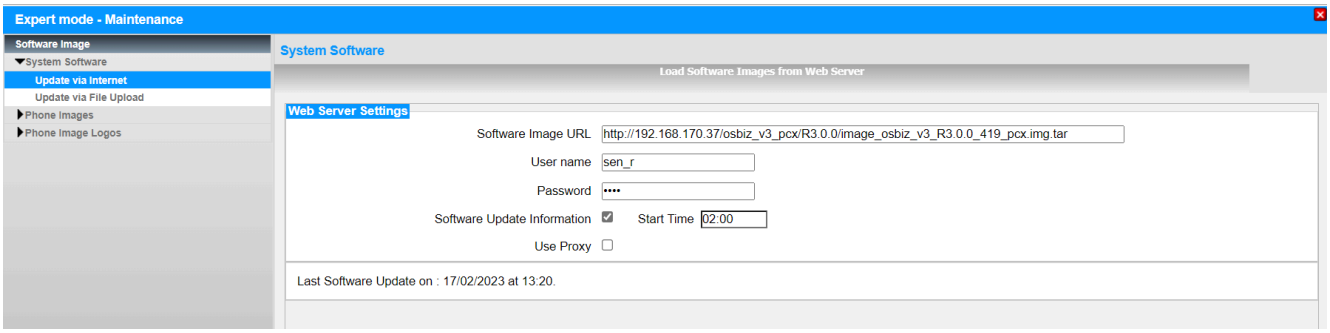
You will need the web address (URL) and the account information to access the local web server as well as the name of the image file.

The image file is stored on the local web server as a tar file, and the storage location is known. The tar file may possibly need to be unpacked from the stored tgz file.

If you use a proxy server for the update, you will also need its data (as well as the user name and password, where applicable).

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click **System Software** in the menu tree.
4) Click on **Update via Internet**.



5) Set up access to the local web server:
   a) Enter the address of the local web server, including the path and name of the image file, under **Software Image URL**.

      NOTICE: The **Default** button can be used to reset the entered values back to their defaults.

   b) Enter the user name and password required to access the local web server in the **User Name** and **Password** fields.
   c) Select the **Software Update Information** check box and enter the time at which the server specified above should be searched for newer software under **Start Time**.
   d) If you are using a proxy server for the transfer, enable the **Use Proxy** check box and enter the data for the proxy server.
6) Click on **Apply**. The entered access data of the local web server is set as the default.

   Is a new image file is already available on the local web server, the software update is initiated, and the license agreement appears (see How to Update the System via a Web Server). The launch of the software update can, however, also be prevented if required.

25.3.2 Updating the Communication System

Updating the communication system includes updates to not only the software of the communication system itself, but also the software images of the system

phones, which are stored on the communication system. A full update of all system components can thus be quickly and easily performed.

Before each software update, the configuration data of the communication system must be backed up (Backup and Restore).

Updating via a Web Server

When performing a software update via a web server, the software server (Internet web server) is accessed by default.

If a local web server is being used, the image file must be stored on the local web server.

For a communication system without a UC Booster Card, it does not matter if an image file for a system with or without a UC Booster Card is used. Only the necessary components are installed.

The system checks for the presence of new software updates after automatically setting up a connection to the web server. For systems without UC Booster, individual software update packages can be unselected to reduce the download time. Only those packages that have changed with respect to the installed software version are transferred. The starting time for the software transfer and for the software activation can be selected. If the time of the software activation is reached before the software update has been completely transferred to the system, the activation is not executed automatically. A new time of activation must then be defined manually.

Updating via USB Storage Device

The image file is stored on a USB device. The USB storage device must be inserted in the USB server port of the communication system. This type of update can only be performed by an administrator with the **Expert** profile and is not possible for OpenScape Business S and OpenScape Business UC Booster Server.

Updating via a File Upload

The image file is in a directory in the internal network or on the admin PC.

Update via a USB Device without WBM Access

The communication system can be updated directly without WBM access via a USB device. This requires the USB device to be plugged into the USB server port of the system and the image file to be located at the top level of the USB device. If a reset of the communication system is performed with the USB device inserted, the software update is started automatically. This type of update is not possible with OpenScape Business S. In a system with the OpenScape Business UC Booster Server, the server must be updated additionally.

Updating the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, then the communication software of the UC Booster Server must also be updated when updating the system software. In other words, the software of the communication system and the UC Booster Server should always be at the same level. The software update of the UC Booster Server is basically identical to the software update for the communication system; the only difference is that

the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

25.3.2.1 How to Update the System via a Web Server

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

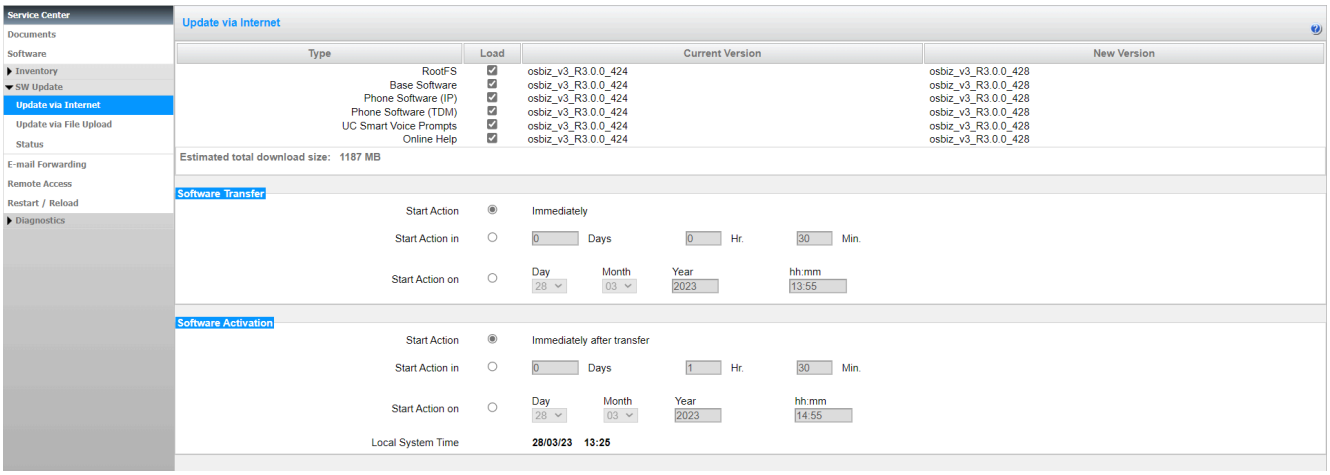
The availability of a new software version is indicated on the home page of WBM.

Access to the web server is available. By default, the connection to the Internet web server is set up. Instead, a local web server can also be configured. (see Using a Local Web Server).

If the update is to be performed via a local web server, the latest image file must be stored on the local web server.

Step by Step

1) Click in the navigation bar on **Home** and then on **Details on the contents can be obtained from here: Link**. This will open a PDF file containing important information about the new software version. Read through the information and pay attention to the information about upgrading the system. Then close the window.
2) Click on **Service Center** in the navigation bar.
3) In the navigation tree, click on **Software Update** > **Update via Internet**. The currently installed software version is displayed to you.
4) Click on **OK & Next**.
5) Read the license agreement (EULA) fully and then enable the radio button **I accept the license agreement**.
6) Click on **OK & Next**.



7) Disable the packages that should not be updated in the **Load** column if required. This is useful with slow Internet connections, for example, or software upgrades via ISDN.
8) Select the times for the software transfer and software activation:
   - **Start Action - Immediate/Immediately after transfer**: The software will be transferred immediately and activated immediately after the

transfer. The software update will be loaded into the communication system in the background. After two restarts, the software is up-to-date.

- **Start Action in**: The software will be transferred and activated after a certain time period. Enter the time period for this in days, hours and minutes.
- **Start Action on**: The software will be transferred and activated at a specific point in time. Enter the date and time for this point in time.

NOTICE: If the time of the software activation is reached before the software update has been completely transferred to the system, the activation is not executed automatically. A new time of activation must then be defined manually.

9) Click on **OK & Next**. The software update will be loaded into the system in the background and activated at the respective times you have configured. Two restarts are automatically performed one after the other for software activation.

NOTICE: You can close the browser window at any time.

10) You can check the current status of the update with the WBM under **Service Center** > **Software Update** > **Status**.

25.3.2.2 How to Update the System using a USB Storage Device

Prerequisites

You are logged into the WBM with the **Expert** profile.

The USB storage device must be formatted with FAT32.

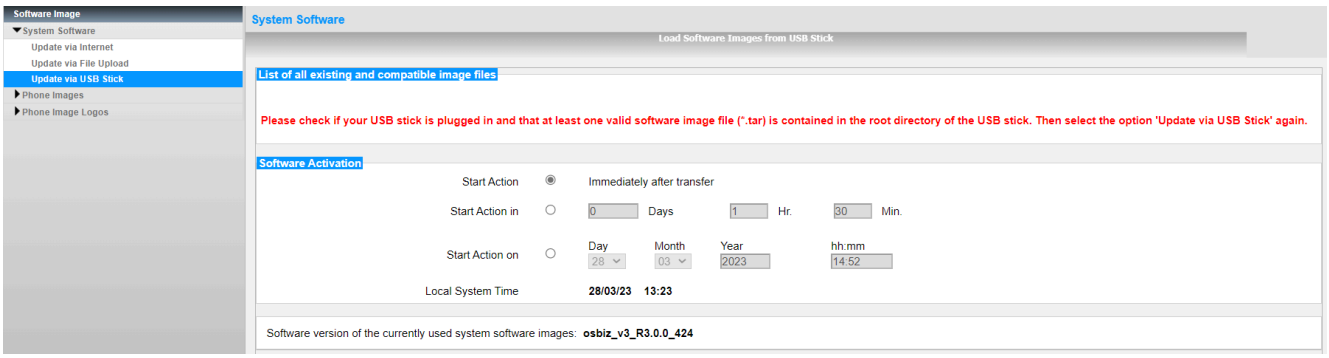
A current image file is stored as a tar file on the USB storage device. It is also possible to have multiple image files stored in different directories.

If the USB storage device has multiple partitions, the image file must be stored in the first partition.

Step by Step

1) Insert the USB storage device into the USB server port on the motherboard.
2) In the navigation bar, click on **Expert Mode**.
3) Click **Maintenance** > **Software Image** in the navigation tree.
4) Click **System Software** in the menu tree.

5) Click on **Update via USB Stick**. All valid image files stored on the USB device are displayed with their respective version number and file name.



6) If multiple image files are stored, select the desired image file; otherwise, the image file is automatically selected.

7) Select the software activation time.

- **Start Action - Immediately after transfer**: The software is activated immediately after it has been transferred to the communication system.
- **Start Action in**: The software is immediately transferred to the communication system. After a specified time, the software is activated. Enter the time period for this in days, hours and minutes.
- **Start Action on**: The software is immediately transferred to the communication system. The software is activated at a specified time. Enter the date and time for this point in time.

8) Click on **Load**. The image file is transferred to the communication system and checked for consistency. Several minutes are required for both processes. During this time, the USB device remain plugged in.

9) Unplug the USB device when instructed by the WBM and then click **Finish**. Two restarts are automatically performed one after the other at the time specified for the software activation.

10) You can check the current status of the update with the WBM under **Service Center** > **Software Update** > **Status**.

25.3.2.3 How to Update the System via File Upload

Prerequisites

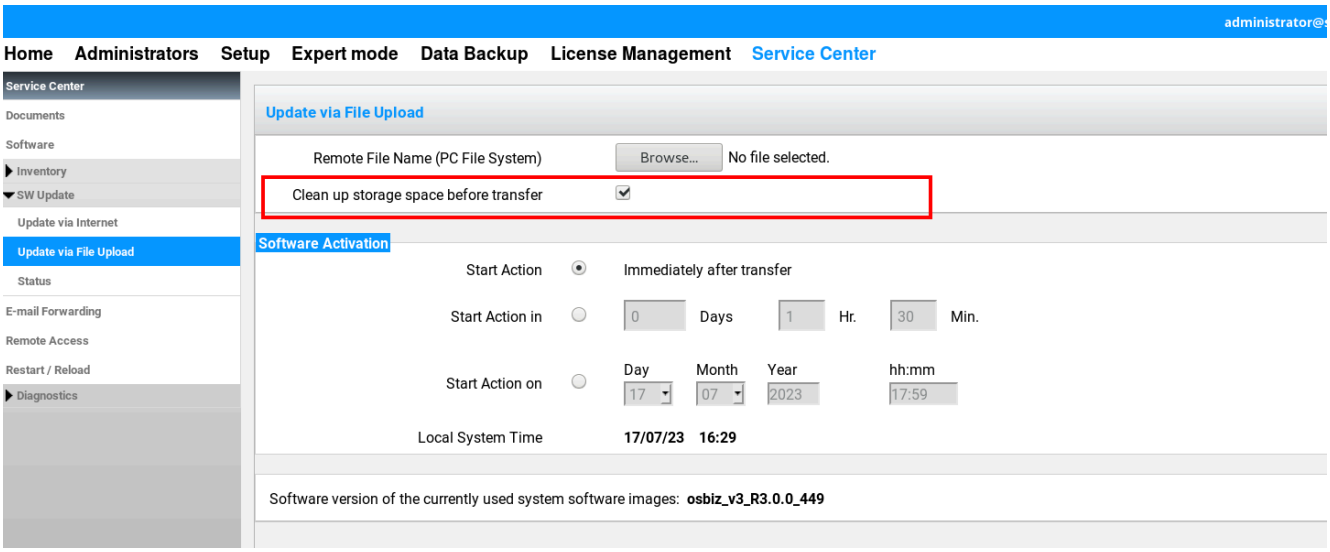
The image file is stored on the internal network or directly on the Admin PC as a tar file, and the storage location is known. If a .tgz file is stored, the tar file must be extracted from the .tgz file.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) In the navigation tree, click on **Software Update** > **Update via File Upload**. The currently installed software version is displayed to you.

3) Click on **OK & Next**.



4) Click the **Browse** button to navigate to the storage location of the image file (`*.tar`).

5) The flag **Clean up storage space before transfer** is enabled by default. The following actions are triggered, to free storage memory in preparation of the software file upload.

   - All logs and traces are deleted.
   - All phone software images are deleted.
   - Any TCP dumps are deleted.

6) Select the software activation time.

   - **Start Action - Immediately after transfer**: The software is immediately transferred to the communications system in the background. After two restarts, the software is up-to-date.
   - **Start Action in**: The software is immediately transferred to the communications system in the background. After a specified time, the software is activated. Enter the time period for this in days, hours and minutes.
   - **Start Action on**: The software is immediately transferred to the communications system in the background. The software is activated at a specified time. Enter the date and time for this point in time.

7) Click on **OK & Next**.

8) The image file is transferred to the communication system and checked for consistency. Several minutes are required for both processes.

NOTICE: If you close the browser window during the software transfer, the operation is canceled. During the consistency checks, you can continue working with the WBM or close it.

---

9) If the software is to be activated immediately, two consecutive restarts automatically occur after the consistency check has been completed successfully.

10) If the software is not to be activated immediately, click **Stop** after the successful transfer. Two restarts are automatically performed one after the other for software activation.

11) You can check the current status of the update with the WBM under **Service Center** > **Software Update** > **Status**.

25.3.2.4 How to Update the System via a USB Device without WBM Access

Prerequisites

The USB storage device must be formatted with FAT32.

A current image file is stored as a tar file at the topmost directory level of the USB storage device. Only one image file may be stored there.

If the USB storage device has multiple partitions, the image file must be stored in the first partition.

The software version of the image file must be newer than the software version of the system. Caution: It is also possible to "update" to older versions of the software.

The communication system has been started.

Step by Step

1) Insert the USB storage device into the USB server port on the motherboard.
2) Press the reset button for 1 to 4 seconds. The system shuts down and initiates a restart.

   During startup, the software is checked. If the USB device contains a suitable image file, the file is uploaded to the communication system. The red LED will flash at 1Hz (0.5 sec on / 0.5 sec off). Upon completion of the copy operation, the software is unpacked, and the customer data is automatically transferred. During this process, the red LED flashes in at 5Hz (100ms on / 100ms off).
3) Remove the USB device when the red LED flashes at 5Hz.
4) Finally, the system automatically performs two restarts in succession. When the green LED flashes at 1-Hz intervals (0.5 s on / 0.5 s off), the system is back in operation.

25.3.3 Updating System Telephones

The software of the system telephones is updated via an image file. For each type of system telephone, there is a separate image file that contains the phone software of this type. These image files are included in the software of the communication system and are automatically loaded into the communication system during updates.

The IP system telephones are thus automatically supplied with the current software. Whenever an IP system telephone is reconfigured in the WBM (from a **System Client** to a **SIP Client**, or vice versa), the appropriate software stored in the communication system is automatically loaded via the DLI into the IP system telephone. For IP system telephones that were already in operation at the system or at some other system, the factory settings must be first restored (factory reset) before the automatic software update can be performed.

Non-standard phone software can be transferred manually by the administrator to all IP system telephones of a specific type by using the WBM. The update of the software for UP0 system telephones is performed with Manager E.

If some specific phone software (image file) is flagged as the default in the WBM, the corresponding image will be automatically transferred to every IP system telephone associated with this type whenever that phone logs into the system for the first time.

When updating the software manually, it is important to ensure that the software of the system telephones is compatible with the software version of the communication system (see the Release Notes).

Related concepts

Telephone Logos on page 1169

25.3.3.1 How to Load the Phone Software into the System

Prerequisites

You are logged into the WBM with the **Expert** profile.

The image files are stored on the local network, and the storage location is known. A separate image file is required for each system telephone type.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click **Phone Images** in the menu tree.
4) Click **Load**. A list of all currently existing image files in the communication system is displayed.
5) Click the **Browse** button under **Remote File Name (PC File System)** to navigate to the storage location of the image file (`*.app`).
6) Click on **Load**. The image file is loaded and checked for errors.

   NOTICE: If an error occurs, you will receive an error message. Verify your entries and repeat steps 5 through 6.

7) If the check succeeds, confirm this with **OK**. The image file is added to the list of currently existing update files in the communication system.
8) To load additional image files for other system telephone types, repeat steps 5 through 7.

25.3.3.2 How to Deploy the Phone Software to System Telephones

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.

3) Click **Phone Images** in the menu tree.
4) If you want to deploy a phone image to all system telephones of a specific type:
   a) Click **Deploy**. A list of all currently existing image files in the communication system is displayed.
   b) Select the check box **Deploy** for the desired phone image or images.
5) If you want to deploy a phone image to a particular system telephone:
   a) Click on **Deploy to device**. A list of the system telephones is displayed.
   b) Select the phone image for the desired system telephone or telephones from the **Deployable software** drop-down list.
6) Click on **Apply**.

25.3.3.3 How to Delete the Phone Software

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click **Phone Images** in the menu tree.
4) Click **Load**. A list of all currently existing image files in the communication system is displayed.
5) Select the check box **Delete** in the row of the phone image to be deleted.
6) If you want to delete more phone images, repeat the previous step.
7) Click on **Delete**. All marked phone images will be deleted from the communication system.

25.3.3.4 How to Enable or Disable the Automatic Distribution of the Phone Software

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Software Image** in the navigation tree.
3) Click **Phone Images** in the menu tree.
4) Click **Deploy**. A list of all currently existing image files in the communication system is displayed.
5) If the phone software should be automatically transferred to the system phones, select the **Standard** checkbox in the row of the desired image file (default setting).
6) If the phone software should not be automatically transferred to the system phones, clear the **Standard** checkbox in the row of the desired image file.
7) Click on **Apply**.

25.3.3.5 How to Configure Automatic Re-flashing

Automatic re-flashing is an easy way to flash HFA software only for out of the box or factory reset OpenScape Desk Phone IP 35G Eco and OpenScape Desk Phone CP 100/110/200/205/210/400/600/600E/700/700X/710, using the system's DLI server.

Prerequisites

You are logged into the WBM with the **Expert** profile.

NOTICE: Automatic re-flashing is valid only for out of the box devices (from the factory). Else, the factory settings must be restored on the device ("factory reset") before proceeding to automatic re-flashing.

Step by Step

1) Configure the device with a number and as system client:
   a) In the navigation bar, click on **Expert Mode**.
   b) In the navigation tree, click **Telephony Server> Station> IP Clients**.
   c) Enter the internal number in the **CallNo** field.
   d) Enter the public number in the **DID** field.
   e) Enter a name for the device.
   f) Select **System Client** from the **Type** drop down menu.
   g) Click **Apply.**

2) Set up the DHCP server to send the IP address of the DLI via the DHCP option:
   a) In the navigation bar, click on **Expert Mode**.
   b) In the navigation tree, click **Telephony Server> Network Interfaces> DHCP> DHCP-Server> Edit Global Parameters**.
   c) Check the **Use Internal DLI** option at the **DNS Server** section.

3) Plug in the device and specify the terminal number once the phone is started.

4) The phone is also registered to the DLI database. To verify the device registration:
   a) Click on **Expert Mode** in the navigation bar.
   b) Click **Maintenance> Software Image** in the navigation tree.
   c) Click **Phone Images** in the menu tree.
   d) Click on **Deploy to Device**.

5) Automatic re-flashing starts and loads the HFA software stored in the communication system to the device.

NOTICE: Do not unplug the device during this process.

The device is now configured.

NOTICE: If the device is set to SIP (under **Telephony Server> Station> IP Clients**), it will update to the latest SIP

software, only if the update is available in the corresponding software release.

When a SIP Client is changed to System Client, a manual restart of the phone is needed in order to load the HFA software.

NOTICE: If the re-flashing process is unsuccessful, the factory settings must be restored ("factory reset") on the device.

25.3.4 Software Status

The software status provides information about the software version and the software update.

The following statuses can be displayed:

- Current version of the software
- Newer version available for an update
- Time at which the software update is to be performed
- New software being loaded into the system
- Successful or failure of the loading process

25.3.4.1 How to Check the Software Status

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

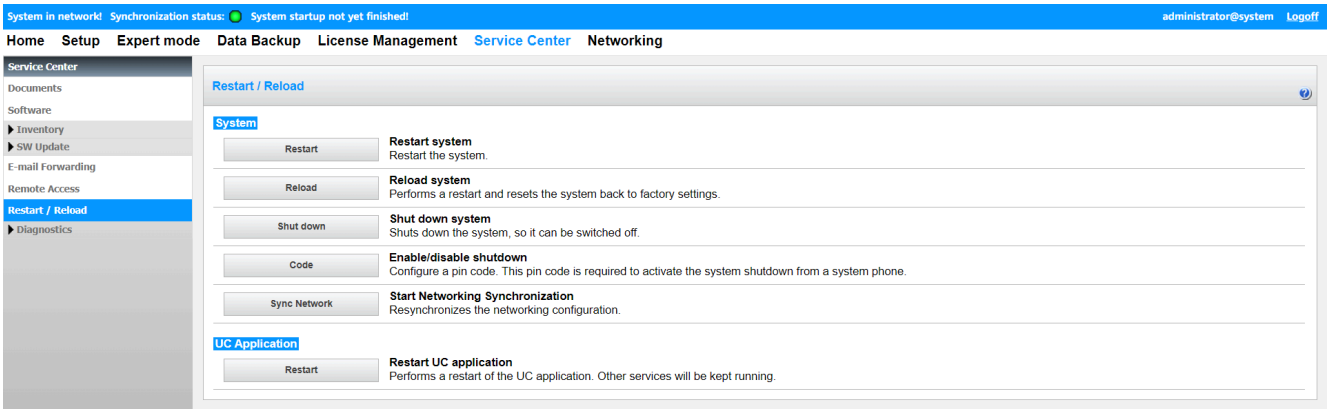
1) Click on **Service Center** in the navigation bar.
2) Click **Software Update** > **Status** in the navigation tree. You will be presented with the latest version of the software. This information is also displayed on the home page of WBM.

   If a software update is running in the background, you will be notified about this here.

   If a new software update is available on the web server, you will be likewise notified about this here. This information is also displayed on the home page of WBM.

25.4 Restart, Reload, Shutdown

You can use the associated features to initiate a restart or reload of the OpenScape Business communication systems or the UC Booster Card and for a controlled shutdown of OpenScape Business X. In addition, a restart (reboot) of the UC application (UC Smart or UC Suite) is triggered. To enable the controlled shutdown of OpenScape Business X via a system telephone, a PIN can be defined.



Restarting and Reloading the UC Booster Server

If a UC Booster Server is being operated in addition to the communication system, the communication software of the UC Booster Server can also be restarted or reloaded. The restart/reload of the UC Booster Server is basically identical to the restart/reload of the communication system; the only difference is that the administrator does not specify the IP address of the communication system when calling the WBM, but the IP address of the Linux server.

NOTICE: See also How to Remove or Delete Unify Phone Users on page 1141.

25.4.1 Restarting OpenScape Business

The **Restart system** function can be used to initiate a controlled restart of OpenScape Business.

The following differences must be observed:

- OpenScape Business S and OpenScape Business X

  A controlled restart of the communication system occurs. The communication system will be operational again after the startup.

  The startup time depends on system configuration and the OpenScape Business networking scenario.

  If OpenScape Business X3/X5/X8 is equipped with a UC Booster Card (Application Board OCAB), a controlled restart (reboot) of the UC Application (UC Smart or UC Suite) also occurs.
- OpenScape Business UC Booster Server (Application Server)

  A controlled restart of the OpenScape Business portion and the UC Application (UC Suite) occurs. The UC Application will be operational again after the startup.

During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

25.4.1.1 How to Initiate a Restart of OpenScape Business

The **Restart system** function can be used to initiate a restart of OpenScape Business.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

INFO: During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Restart system** followed by **OK**. OpenScape Business performs a restart (reboot).

   OpenScape Business S and OpenScape Business X: The communication system will be operational again after the startup.

   OpenScape Business UC Booster Server: After the startup, the UC Application (UC Suite) will be operational again.

25.4.2 Reloading OpenScape Business

The **Reload system** function can be used to initiate a reload of OpenScape Business.

The following differences must be observed:

- OpenScape Business S and OpenScape Business X

  The communication system is reloaded. After the subsequent startup, the communication system will be in its default state.

  – All country and customer-specific settings were deleted (system country code = Germany).
  – The communication system has the default IP address 192.168.1.2 and the internal IP range 192.168.3.xxx.
  – The licensing is retained.

  The startup time depends on system configuration.
- OpenScape Business UC Booster Server

  The OpenScape Business portion is reloaded. After the subsequent startup, the OpenScape Business portion will be in its default state.

  – All custom (i.e., customer-specific) settings of the OpenScape Business portion (e.g., the User Directory) were deleted.
  – The licensing is retained.

  The operating system will not be reset.

25.4.2.1 How to Initiate a Reload of OpenScape Business

The **Reload system** function can be used to initiate a reload of OpenScape Business.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

OpenScape Business S and OpenScape Business X: The configuration data of the communication system was saved in a backup set.

NOTICE:

The reload reverts the communication system to its default state. All country and customer-specific settings are deleted (system country code = Germany). The default IP address (192.168.1.2) of the communication system is reset.

OpenScape Business UC Booster Server: The configuration data of the OpenScape Business portion was saved in a backup set.

NOTICE:

The reload reverts the OpenScape Business portion to its default state. All custom (i.e., customer-specific) settings of the OpenScape Business portion (e.g., the User Directory) are deleted.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Reload system**, followed by **OK**. OpenScape Business reloads.

INFO: OpenScape Business S and OpenScape Business X: After the subsequent startup, the communication system will be in its default state. After the basic settings have been configured using the **Initial Installation** wizard, country- and customer-specific data backups can be reloaded. For more detailed information on the procedure, see Restore .

OpenScape Business UC Booster Server: After the subsequent startup, the OpenScape Business portion will be in its default state. The backed-up customer-specific data can be reloaded. For more detailed information on the procedure, see Restore .

25.4.3 Shutting Down OpenScape Business X

The **Shut down system** function can be used to shut down the OpenScape Business X communication systems gracefully, i.e., to perform a controlled shutdown.

25.4.3.1 How to Shut Down OpenScape Business X

The **Shut down system** function can be used to shut down OpenScape Business X communication systems gracefully, i.e., to perform a controlled shutdown.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Shut down system** followed by **OK**. A controlled shutdown of the communication system is performed.

INFO: OpenScape Business X1/X3/X5: The subsequent startup of the communication system is only possible by unplugging and then reinserting the power plug.

OpenScape Business X8: the subsequent startup of the communication system is only possible by switching off all LUNA2 power supplies and then switching them back on again.

25.4.4 PIN for the controlled shutdown of OpenScape Business X

The activation of the shutdown via a system telephone is PIN-protected.

The PIN configured in the communication system must be entered for the activation via a system telephone. The configuration of this PIN is performed by an administrator with the **Advanced** profile.

25.4.4.1 How to Configure a PIN for the Controlled Shutdown of OpenScape Business X

The PIN is for initiating a shutdown via a system telephone.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Enable/disable shutdown**.
4) Enter the desired six-digit PIN in the **PIN** field.
5) Click on **Save** followed by **OK**.

Next steps

The activation of a shutdown via a system telephone occurs by entering the corresponding code (default code = *997), followed by the six-digit PIN.

- For IP phones: you can execute the controlled shutdown from the first two configured devices.
- For UP0 phones: you can execute the controlled shutdown from each of these phones. In this case, the IP clients do not have rights to execute a shutdown.

25.4.5 Restarting (Rebooting) the UC Booster Card (Application Board OCAB)

As an administrator, you can use the **Restart Application Board** function to initiate a controlled restart of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

In addition, the CSTA interface, the Presence Manager, Announcement Player, Media Extension Bridge and Open Directory Service are likewise restarted.

25.4.5.1 How to Initiate a Restart of the UC Booster Card (OCAB Application Board)

The **Restart Application Board** function can be used to initiate a controlled restart of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

INFO: During a restart, all active applications such as myPortal for Desktop and myPortal for Outlook, for example, are disconnected. After the startup, all connections are automatically set up again.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Restart Application Board** followed by **OK**. The UC Booster Card (Application Board OCAB) performs a restart.

25.4.6 Reloading the UC Booster Card (Application Board OCAB)

The **Reload UC Booster Card** function can be used to initiate a reload of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

The Reload UC Booster Card function is used to reset the card to the factory settings and then remove it from the system. This may be necessary if the card is no longer to be used in this system due to a switch to the UC Booster Server or if it is to be installed in another OpenScape Business system.

All customer-specific data and all diagnostic data are deleted from the UC Booster Card, and the system shuts down. Then, the system must be unplugged from the power supply, and the UC Booster Card must be removed.

After the UC Booster Card has been removed and the system is rebooted, a new backup set must be created, since the configuration data has changed and the old backup set is no longer compatible. If the hard disk of the UC Booster Card was previously used as a backup medium, then another backup medium such as a network drive, a USB device or an FTP/FTPS server must be now selected (see also the Backup and Restore).

25.4.6.1 How to Initiate a Reload of the UC Booster Card (OCAB Application Board)

The **UC Booster Card Reload** function can be used to initiate a reload of the Application Board OCAB, including the UC application (UC Smart or UC Suite).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **UC Booster Card Reload**, followed by **OK**. You are logged out of the WBM. The card is reset to the factory settings, and the system then shuts down.
4) Once the Green RUN LED of the mainboard and the controller LEDs of the UC Booster Card are completely turned off, unplug the system from the power supply and remove the UC Booster Card (see the Backup and Restore).

25.4.7 Restarting the UC Application

The **Restart UC Application** function can be used by an administrator to initiate a controlled restart of the UC Application (UC Smart or UC Suite).

During a restart of the UC Application, all active applications such as myPortal for Desktop and myAttendant, for example, are disconnected. After the startup, all connections are automatically set up again.

25.4.7.1 How to Initiate a Restart of the UC Application

The **Restart UC Application** function can be used to initiate a restart of the UC Application (UC Smart or UC Suite).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

INFO: During a restart, all active applications such as myPortal for Desktop and myAttendant, for example, are disconnected. After the startup, all connections are automatically set up again.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Restart / Reload** in the navigation tree.
3) Click on **Restart UC Application** followed by **OK**. The UC Application performs a restart.

25.5 Inventory Management

The term Inventory Management refers to the process for determining the current status of the OpenScape Business X and OpenScape Business S communication systems and the hardware configuration of the OpenScape Business X communication system.

25.5.1 System Status

The current status of the OpenScape Business X and OpenScape Business S communication systems can be determined by an administrator via the WBM. The following information can be retrieved: status of the stations, connection setup, ITSPs, VPNs and the list of configured IP addresses.

Station status

The station status enables the following information on the configured stations to be retrieved:

- Station number
- Name
- Device type
- IP address (for system telephones, an additional link through which the WBM of the phone can be opened is displayed.)
- MAC Address
- Current SW version
- HW version
- Status (On/Off)

Dial-up Network Status

The dial-up network status enables information on existing connections to PSTN partners (i.e., Public Switched Telephone Network partners such as public or home telecommunications networks, for example) of the OpenScape Business X communication system to be retrieved.

ITSP Status

The ITSP status enables information on the current status of preconfigured and any possibly added Internet Telephony Service Providers (ITSPs) to be retrieved. In addition, it shows which stations were set up for which ITSP.

The status of each active ITSP is indicated by the color of the associated rectangle (green = OK, orange = at least one of the stations was not properly configured).

VPN Status

The VPN status enables information on the configured VPN tunnels of the OpenScape Business X communication system to be retrieved:

Overview of IP Addresses

The IP addresses configured in the OpenScape Business X communication system are displayed.

In addition, the overview also shows with which wizards and with which menus in Expert mode the IP addresses can be configured.

Also, a status overview of the Booster Card and the Mainboard Ethernet Interfaces is displayed.

25.5.1.1 How to Check the Station Status

The **Status** wizard can be used to determine the current status of all configured stations.

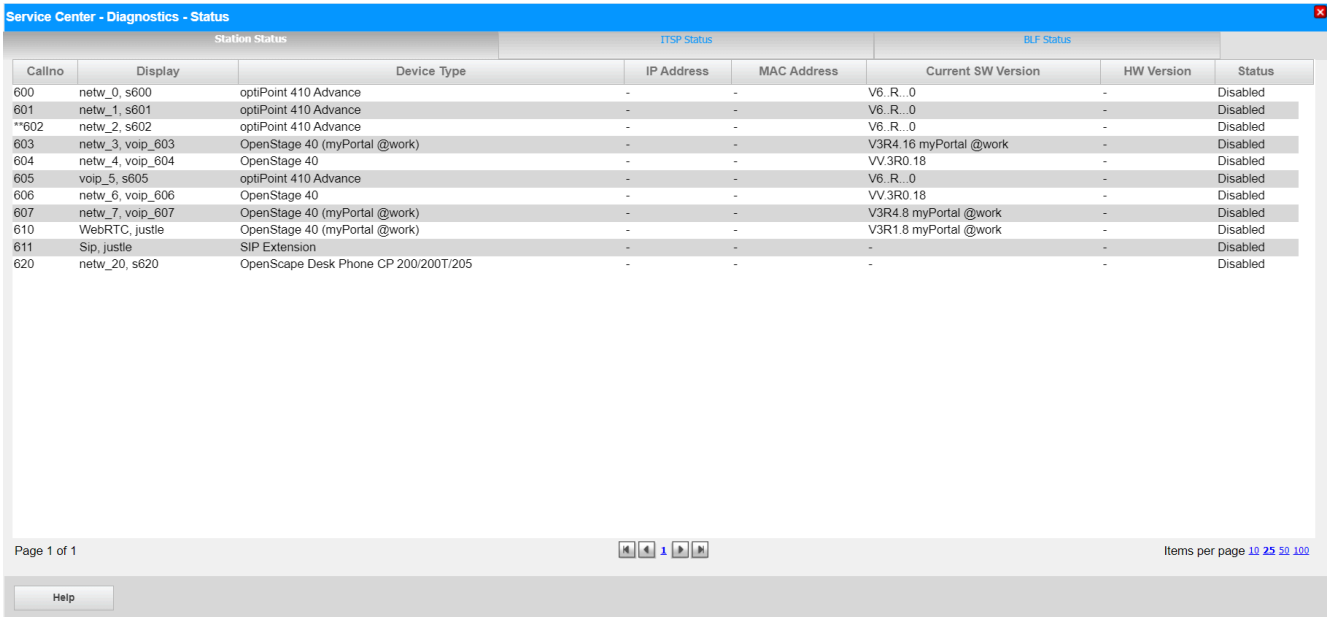
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Status** in the navigation tree.

3) Click on the **Station Status** tab. The status of all configured stations is displayed.



4) Click on **Finish**.

25.5.1.2 How to Check the Status of the Connection Setup

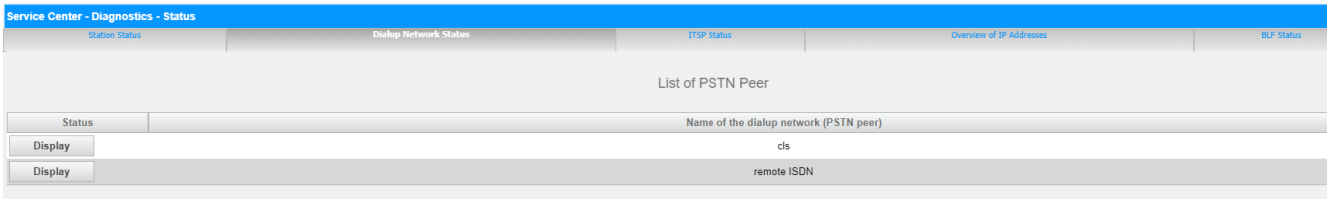
The **Status** wizard can be used to determine the current status of the PSTN peers of an OpenScape Business X system.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Status** in the navigation tree.
3) Click on the **Dialup Network Status** tab. The list of PSTN peers is displayed.
4) Click in the row of the desired connection (PSTN peer) on **Display**. The current status of this connection (PSTN peers) is displayed.



5) If you want to retrieve the status information of a further connection (PSTN peer), continue as described under Step 3.
6) Click on **OK** followed by **Finish**.

25.5.1.3 How to Check the ITSP Status

The **Status** wizard can be used to determine the current status of the Internet Telephony Service Provider (ITSP).

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Status** in the navigation tree.
3) Click on the **ITSP Status** tab. The current status of the preconfigured and any possibly added Internet Telephony Service Providers (ITSPs) in active status is displayed.
4) Click on **Diagnose** to get additional information about the SIP connection.
5) Click on **Finish**.

25.5.1.4 How to Display IP Addresses

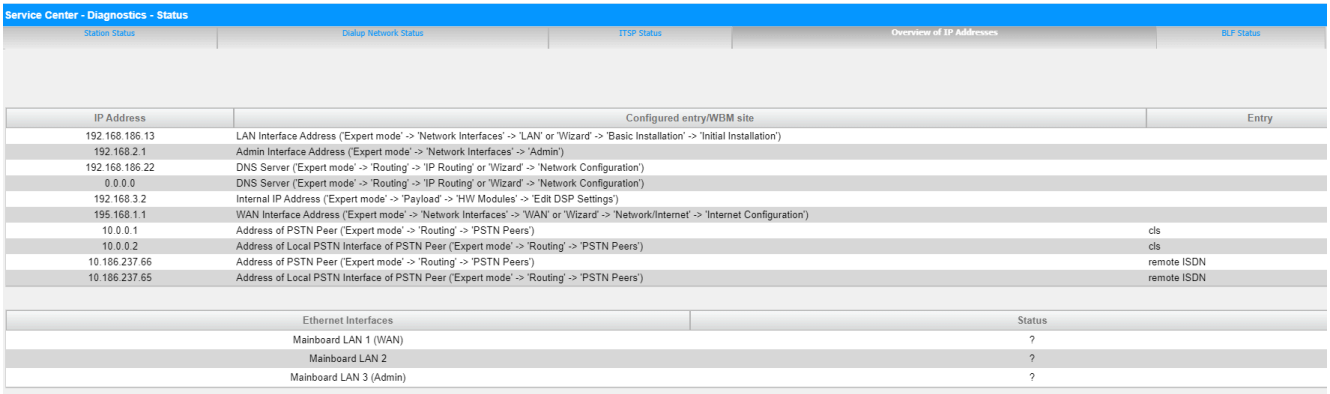
The **Status** wizard can be used to obtain an overview of the IP addresses configured in an OpenScape Business X communication system. In addition, the overview also shows with which wizards and with which menus in Expert mode the IP addresses can be configured.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Status** in the navigation tree.
3) Click on the **Overview IP Addresses** tab. An overview of the IP addresses configured in the communication system is displayed.



4) Click on **Finish**.

25.5.2 Inventory

The Inventory enables an administrator to retrieve information on the hardware and software of OpenScape Business X and the software of OpenScape Business S.

OpenScape Business X

The following details can be retrieved:

- Communication system

  Among other things, the following information is displayed:

  – Graphical representation of the communication system and the boards
  – Part number of the mainboard, MAC address, IP address, host name and software version
  – Type of the CPU and RAM (in GB) of the system
  – Details on memory amounts, including the available and used space on the SDHC card
  – Status of all applications
- Boards

  The displayed information includes the following: slot, type, part number and status of all installed boards.
- UC Booster Card (Application Board OCAB), if available

  Among other things, the following information is displayed:

  – MAC address, IP address, host name and software version
  – Details on memory amounts, including the available and used hard disk space.
  – Status of all applications
  – Overview of all Booster Card interfaces

  The link **UC Booster Card accessible** in the home page of WBM directs the user to the **Service Center > Inventory >Booster Card** for a detailed view. The link will exist, even if there is a problem with the Booster Card and the text shows **UC Booster Card not accessible**.

  The following error messages are displayed in the home page of WBM, depending on the error:

  1) Inter-Integrated Circuit link with Booster Card not possible
  2) Internet Protocol v6 connectivity to Booster Card not possible
  3) Internet Protocol v4 connectivity to Booster Card not possible
  4) Secure Socket Shell connectivity to Booster Card not possible
  5) Network File System connectivity to Booster Card not possible
  6) One or more Ethernet Interfaces are in Half Duplex mode, Full Duplex is highly recommended

OpenScape Business S

The following details can be retrieved:

- Software

  Among other things, the following information is displayed: MAC address, IP address, host name and software version.
- Hard Disk Information

  Details on memory amounts, including the available and used memory.
- Applications

  All applications and their respective statuses are displayed.

25.5.2.1 How to Check the Inventory of OpenScape Business X

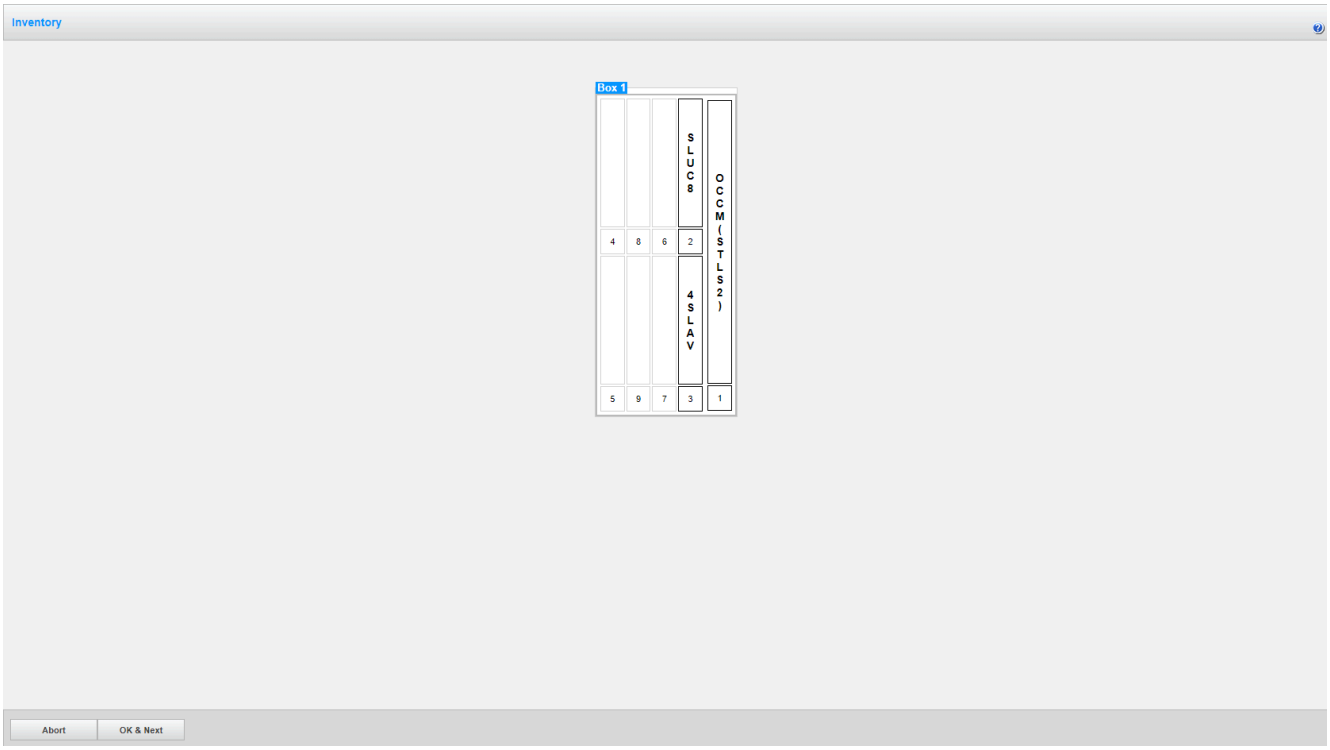
The **Inventory** wizard can be used to determine the current status of the hardware and software of the OpenScape Business X communication systems.

Prerequisites

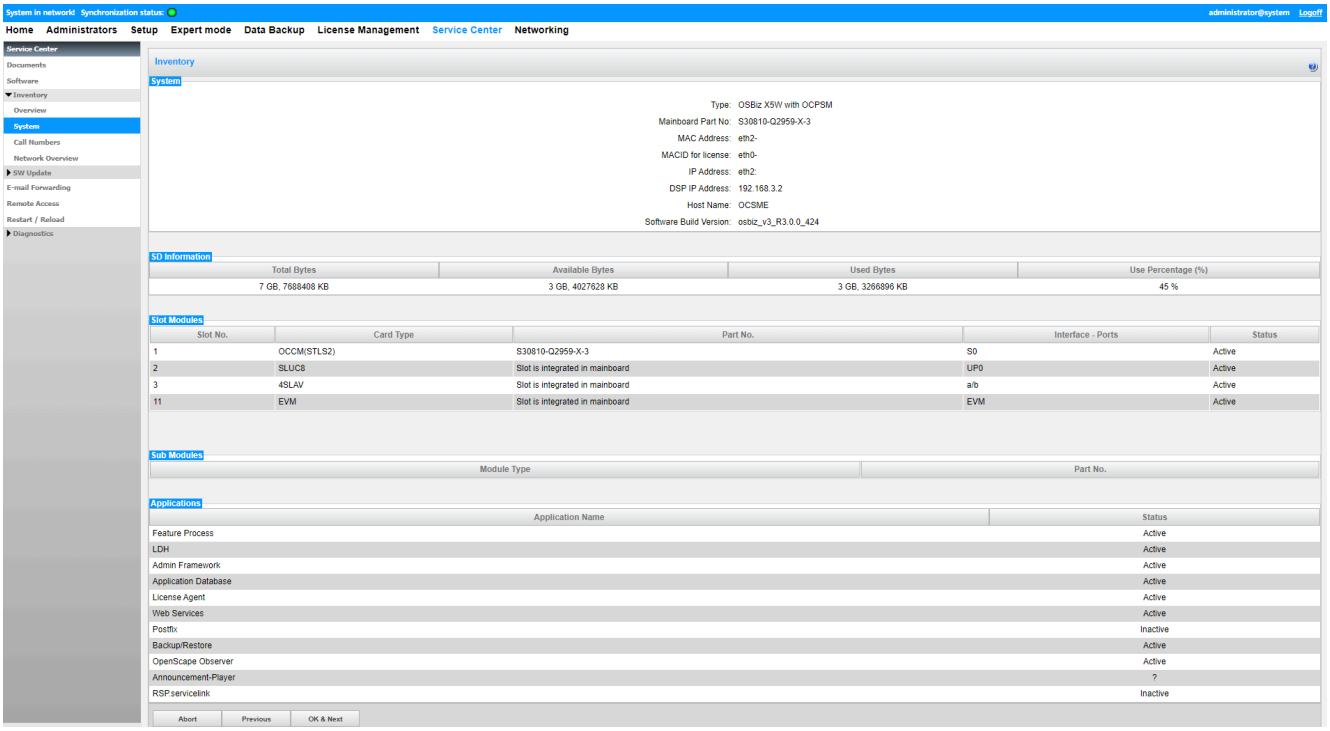
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) In the navigation tree, click **Inventory** > **Overview**. You will be shown a graphical representation of the communication system and the boards.



3) Click on **OK & Next**. Information on the communication system, the available and used space on the SDHC card, the boards and the application status will be displayed.



4) Click on **OK & Next**. The subsequently displayed information depends on whether or not the communication system is equipped with a UC Booster Card (Application Board OCAB):

   a) If your communication system is not equipped with a UC Booster Card: Information on the assignment of call numbers to the boards is displayed.

   b) If your communication system is equipped with a UC Booster Card: Information on the OCAB Board, on the available and used storage space on the hard drive and on the application status and on the status of the Booster Card interfaces is displayed.

   Click on **OK & Next**. Details on the allocation of call numbers to the boards will be displayed.

5) Click on **Finish**.

25.5.2.2 How to Check the Inventory of OpenScape Business S

You can check the current status of the OpenScape Business S software with the **Inventory** wizard.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) In the navigation tree, click **Inventory**. Information on the software of the communication system, the available and used hard disk storage and on the application status will be displayed.

25.6 Automatic Actions

This function can be used to define actions to be executed once or at regular intervals. These actions are then executed automatically by the communication system at the set time.

25.6.1 Garbage Collection Automatic Action

The automatic action Garbage Collection enables an automatic garbage collection to be performed on the communication system. After each garbage collection has been completed, the communication system performs a restart (reboot).

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

Start/Stop Action can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action Garbage Collection is disabled by default.

25.6.1.1 How to Edit the Garbage Collection Action

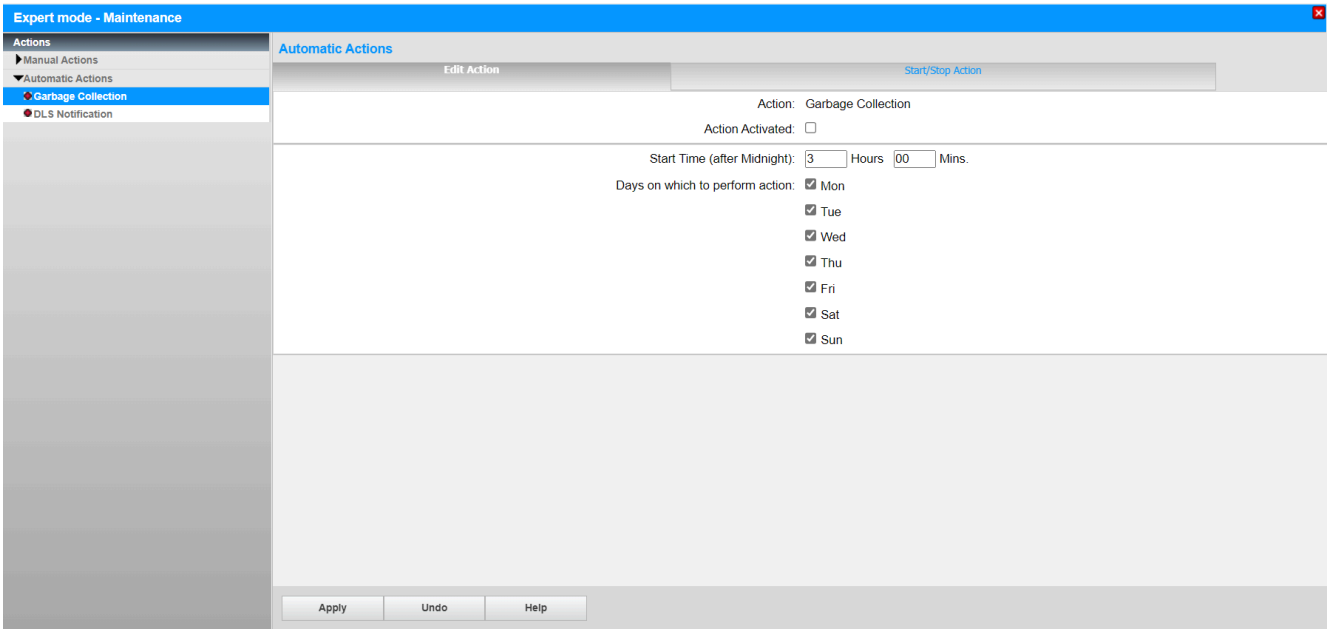
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click on **Actions** > **Automatic Actions** > **Garbage Collection** in the menu tree.

4) Click on the **Edit Action** tab.



5) Select the desired setting.

- If you want the Garbage Collection action to be performed, select the **Action Activated** check box.
- If you do not want the Garbage Collection action to be performed, clear the **Action Activated** check box.

6) If appropriate, change the **Start Time (after Midnight)**.

Enter the number of hours in the **Hrs** field and the number of minutes in the **Mins** field to indicate the interval after which the action should be executed.

Example: Let us assume that the values entered in the **Hrs** field was `3` and in the **Mins** field was `30`. This means the garbage collection action will be performed at 3:30 a.m. every morning.

7) If required, change the weekdays via **Days on which to Perform Action**.

Enable the check boxes of the weekdays on which the action is to be performed. Clear the check boxes of the weekdays on which the action is not to be performed.

8) Click on **Apply** followed by **OK**.

25.6.1.2 How to Start the Garbage Collection Automatic Action (Activate)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click on **Actions** > **Automatic Actions** in the menu tree. The names of all automatic actions are displayed in the menu tree. Disabled actions are flagged with a red bullet point. Enabled actions are flagged with a green bullet point.

4) Click **Garbage Collection** in the menu tree.
5) Click on the **Start/Stop Action** tab.
6) Click on **Start** followed by **OK**.

25.6.1.3 How to Stop the Garbage Collection Automatic Action (Deactivate)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click on **Actions** > **Automatic Actions** in the menu tree. The names of all automatic actions are displayed in the menu tree. Disabled actions are flagged with a red bullet point. Enabled actions are flagged with a green bullet point.
4) Click **Garbage Collection** in the menu tree.
5) Click on the **Start/Stop Action** tab.
6) Click on **Stop** followed by **OK**.

25.6.2 DLS Notification Automatic Action

The automatic action DLS Notification can be used to initiate an automatic login at an external DLS server on starting up the communication system.

The color of the list item displayed in the menu tree indicates the status of the action (green = action activated, red = action not activated).

Start/Stop Action can be used to enable or start an inactive action (red list item) and to disable or stop an active action (green bullet point).

The automatic action DLS Notification is disabled by default.

25.6.2.1 How to Edit the DLS Notification Automatic Action

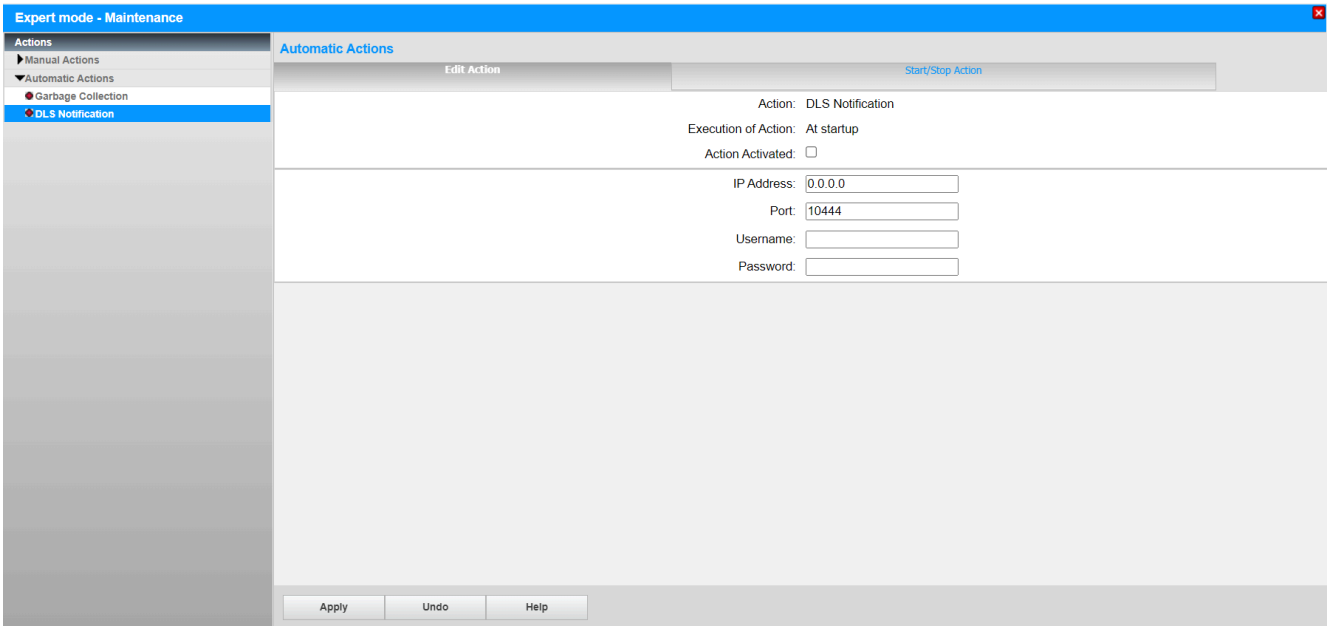
Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click in the menu tree on **Actions** > **Automatic Actions** > **DLS Notification**.

4) Click on the **Edit Action** tab.



5) Select the desired setting.
   - If you want the DLS Notification action to be performed, select the **Action Activated** check box.
   - If you do not want the DLS Notification action to be performed, clear the **Action Activated** check box.
6) If appropriate, change the IP address of the external DLS server in the **IP Address** field.
7) If appropriate, change the port of the external DLS server in the **Port** field.
8) If appropriate, change the user name for logging on to the external DLS server in the **User name** field.
9) If appropriate, change the password for logging on to the external DLS server in the **Password** field.
10) Click on **Apply** followed by **OK**.

25.6.2.2 How to Start the DLS Notification Automatic Action (Activate)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click on **Actions** > **Automatic Actions** in the menu tree. The names of all automatic actions are displayed in the menu tree. Disabled actions are flagged with a red bullet point. Enabled actions are flagged with a green bullet point.
4) Click **DLS Notification** in the menu tree.
5) Click on the **Start/Stop Action** tab.
6) Click on **Start** followed by **OK**.

25.6.2.3 How to Stop the DLS Notification Automatic Action (Deactivate)

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Actions** in the navigation tree.
3) Click on **Actions** > **Automatic Actions** in the menu tree. The names of all automatic actions are displayed in the menu tree. Disabled actions are flagged with a red bullet point. Enabled actions are flagged with a green bullet point.
4) Click **DLS Notification** in the menu tree.
5) Click on the **Start/Stop Action** tab.
6) Click on **Stop** followed by **OK**.

25.6.3 Warning Mechanism for SDHC card lifetime

The automatic action Warning Mechanism for SDHC lifetime is a way to get information about the SDHC cards health state with a filesystem check during startup. A WBM wizard starts and leads the technician through the process of setting a time when the system should make a restart and execute the check.

NOTICE: In case that no filesystem errors are found by the check, **Card Health Status** will be set back to green or yellow even if errors were reported before.

All information is logged in the Customer Trace. The automatic action Warning Mechanism for SDHC is disabled by default

---

NOTICE: This option triggers a system restart while prompting an Alert box "`Note: System will restart soon after you press OK.`"

WBM Home Screen recognizes two states:

- If the information from system is available a text will be presented in Home Screen informing about the general status of the card, **Card Health Status** (green, yellow, red or grey).

  The general lifetime of the card is calculated based on the manufacturer specifications and the average writing cycles of the system. Different values for card lifetime are possible.This information is presented together other information at the SDHC Health check page within the WBM.

  An estimated lifetime of 4 years for standard cards and 10 years for high endurance cards are stored within the system.

  NOTICE: The estimated values for the lifetime are only the base for the intergrated Card Health Status Warning

Mechanism. These values do not imply automatically that a card is defect after this time is expired.

Green health status means that the card has not reached its estimated lifetime and there is no problem with the filesystem.

Yellow health status means that the card has reached its estimated lifetime.

Red health status means that there are over 50 filesystem errors detected.

Grey health status means that the card is not supported or that it is not possible to retrieve card information. The SDHC card must be replaced by a supported type.

The Warning Mechanism for Yellow health status is based on the manufacturing date and the estimated lifetime of the card. As cards can be in stock for longer time until they are used within OpenScape Business, the filesystem creation date is also considered within the calculation algorithm.

Below a calculation table is shown for Card Health Status with an estimated lifetime of 4 years.

Factor	Years and Weight									
Manufacturing Date	< 4 years	< 5 years		< 6 years		< 7 years		< 8 years		> 8 years
Filesystem Created	< 4 years	< 4 years	4-5 years	< 4 years	4 - 6 years	< 3 years	3-7 years	< 2 years	2 - 8 years	-
Health Status	Green	Green	Yellow	Green	Yellow	Green	Yellow	Green	Yellow	Yellow

- If the information is not available then user will be prompted, **Card Health Status** unknown.

NOTICE: In case that the file system is corrupted the appropriate System SW image has to be downloaded from SWS and has to be copied to the SDHC card using the Card Manager Tool. After starting up the system with the new SDHC card, the configuration can be restored using the latest backup.

The text "**Card Health Status** " will also provide a link that will leads to the "Actions Page"

25.6.3.1 How to set a notification in case of errors in SDHC card

In case that the integrated filecheck function reports a number of errors which exceeds the given threshold (50 errors) or the system cannot read/write any longer from/to the SDHC Card during normal operation, the system notifies with an E-Mail or an SNMP event.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Reaction Table** in the menu tree. The names of Reaction Table are displayed in the menu tree.
4) Select **FP_EVT_HW_067** in the menu tree.
5) Select one of the following available options:
   a) Send an SNMP Trap.
   b) Send an E-mail.
6) Click on **Apply** followed by **OK**.

NOTICE: The e-mail address needs to be configured in **Expert mode > Maintenance > Events > E-mail.**

25.6.3.2 How to Start the Warning Mechanism for SDHC lifetime Automatic Action

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) Save the system with the Backup function to an external medium.
2) In the navigation bar, click on **Expert Mode**.
3) Click **Maintenance** > **Actions** in the navigation tree.
4) Click on **Actions** > **Automatic Actions** in the menu tree. The names of all automatic actions are displayed in the menu tree.
5) Click **SDHC Health Check** in the menu tree.

   Date and time of **Local System Time** and **Last Health Check** are displayed.The content of **log file** is also displayed.
6) Select one of the following available options:
   a) Start Health Check immediately.
   b) Start Health Check on a specific date
7) Click on **Apply** followed by **OK**.

25.6.3.3 How to clone and change an SDHC card

SDHC cards have a limited lifetime in general. The lifetime depends mainly on the number of writing cycles of the SDHC card. OpenScape Business supports an integrated "SDHC Health Status" detection mechanism for the lifetime of the SDHC card and an integrated "SDHC Data Backup" function, which is described below for the replacement of the exhausted SDHC card and the creation of a new and full functional card.

NOTICE: The SDHC Data Backup function is able to copy the content of the SDHC card that is currently inserted in the system without shutting down the system. See also How to Remove or Delete Unify Phone Users on page 1141.

The relevant data can be backed-up to different storage locations and storage media as:

- USB stick connected to the system.
- USB SDHC card reader connected to the system.
- Network File System (NFS) drive.
- Network File System (NFS) drive via USB.

NOTICE: The USB stick or USB SDHC card reader options are not available for OpenScape Business X1. In this case, the SDHC data backup needs to be stored to a NFS drive.

In case where a USB card reader is used, the possibility of the SDHC card for not accessing or formatting cannot be excluded. In this case, another USB card reader or a USB stick should be used.

In case that a USB card reader with the new inserted SDHC card is used and is directly connected to the system, the integrated SDHC Data Backup function creates a full functional SDHC card. In all other cases, it creates a so-called "tar file" which contains all the system and configuration data.

NOTICE: The tar file cannot be used by the restore function of the system.

The size of SDHC Data Backup (tar file) depends on the specific data of the system and it can increase to multiple GB if media files (voicemails, call records etc.) are stored.

In order to clone and change a SDHC card in a live system, the following procedure is required:

1) Create a SDHC Data Backup File with a suitable media (see How to create a SDHC Data Backup File)
2) Create a new operational SDHC card including all system data (see How to Use the Card Manager to Write the Communication Software on the SDHC Card on page 1278).
3) Power off the system, change the SDHC card and power on again (See How to Use the Card Manager to Write the Communication Software on the SDHC Card on page 1278).

25.6.3.4 How to create a SDHC Data Backup File

Prerequisites

A USB stick with at least the same capacity as the SDHC card of the system or a USB card reader with a new, inserted SDHC card with at least the same size as the card of the system or a Network File System (NFS) drive which is accessible from the system.

Step by Step

1) In the navigation bar, click on **Data Backup**.
2) Click **SDHC Data Backup** > **Data Backup** in the navigation tree.

3) Select one of the following available options depending on the available storage location and media:

a) NFS

A valid server address, the relevant path and valid login credentials must be configured.

Click on **Save & check**

NOTICE: A Scheduled Backup is available. Only one action can be scheduled at a time and the user will be able to change it or cancel it.

---

b) Card Reader

This option creates a full functional copy of the SDHC card without trace and log files.

A USB SDHC card reader with an inserted SDHC card must be plugged in the system before the copy process is started.

After the process begins, the inserted SDHC card is formatted and all relevant files are transferred to the inserted SDHC card.

NOTICE: Do not remove the USB SDHC Card reader or the inserted SDHC card before the process is finished.

NOTICE: The new SDHC card is full functional for immediate use in the OpenScape Business system. The

new card contains all files and data except log and trace files.

NOTICE: A Scheduled Backup is available. Only one action can be scheduled at a time and the user will be able to change it or cancel it.

c) NFS via USB.

A valid server address, the relevant path and valid login credentials must be configured.

Click on **Save & check**

NOTICE: A Scheduled Backup is available. Only one action can be scheduled at a time and the user will be able to change it or cancel it.

d) USB.

A FAT32 formatted blank USB device has to be plugged in the system.

NOTICE: Do not remove the USB stick before the process is finished.

NOTICE: The copied SDHC Backup data file (tar file) can be used in the Card Manager Tool to create a full functional SDHC card for the system.

NOTICE: A Scheduled Backup is available. Only one action can be scheduled at a time and the user will be able to change it or cancel it.

4) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.

NOTICE: An error message appears if the NFS share or the USB cannot be mounted or if the storage media cannot be formatted.

5) The message **Backup task was finished successfully** is displayed after the backup file is successfully copied.

6) Click on **Finish**.

NOTICE: Depending on the chosen storage location and media, the further procedure differs.

In case of using the SDHC Card Reader with SDHC card, the new SDHC card can immediately be used.

In all other cases, the generated SDHC Card Backup file has to be used in combination with the Card Manager tool to generate a new SDHC card.

Next steps

Follow the steps to create a new operational SDHC card and change it in the live system (see How to Use the Card Manager to Write the Communication Software on the SDHC Card on page 1278)

25.6.3.5 How to replace an SDHC Card

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Only when using UC Suite: UC Suite has started correctly.

Downgrade to previous software version is not supported. If a card with V2 software is installed, then only previous minor releases of V2 can be restored.

The current Software version has to be used in order to avoid any side effect.

NOTICE: In case the SDHC card is broken and the system is down a previous backup should be used and the first 10 steps of the following procedure should be ignored. See also How to Remove or Delete Unify Phone Users on page 1141.

Step by Step

1) Click on **Backup and Restore** in the navigation bar.
2) In the navigation tree, click **Backup - Immediate.**
3) Enter a comment for the backup set in the **Comment** field so that the backup set can be easily identified if needed later for a restore. Avoid the use of diacritical characters such as umlauts and special characters in your input.
4) If you want to create a backup set including voice messages an announcements, select the **Full Backup** option.
5) Activate the target drive on which the backup set is to be saved in the **Devices** area.
6) Click on **OK & Next**. The progress of the backup process is displayed in aseparate window.

NOTICE: If the **OK & Next** button is grayed out, then one or more applications (e.g., UC Suite) for which the data is to be saved were not started correctly.

If you do not have access rights for the selected archive directory, you will receive an error message. Select another destination drive or change the path for the archive.

An error message appears if there is not enough disk space on the destination drive for the backup set. If this occurs, select another destination drive or delete a backup set and restart the backup.

NOTICE: If you are using a USB device as a backup medium, wait till the LED of the USB device stops flashing.

It is only then that the backup has been successfully stored on the USB device. You can then remove the USB device.

NOTICE: In addition to backup set, a text file associated with the backup set must also be saved. It contains information about the date and time of the backup and under which software version the backup was performed.

---

7) The backup was successful if the message **Backup completed successfully! 100%** appears.
8) If you have selected **HTTPS** as a backup medium, you must save the backup set and the text file associated with the backup to a location of your choice. This is done automatically for the other backup media. The browser window must remain open until the save operation for the backup set and text file has been completed.
9) Click on **Finish**.
10) Switch off the system.
11) Remove the existing SDHC card.
12) Install the new SDHC card.
13) Switch on the system.

    When a new SDHC card is installed, the software version included to the card with the default configuration is automatically installed to the system.After Startup, system will have it's default IP address.
14) Click on **Backup and Restore** in the navigation bar.
15) Click **Restore** in the navigation tree.
16) Activate the medium containing the backup set to be restored in the **Devices** area.
17) If you activated **HTTPS** as the backup medium, navigate to the storage location of the backup set and select the backup set. Then navigate to the storage location of the text file and select it.
18) If you activated any other backup medium than **HTTPS**, select the backup set containing the configuration data to be restored in the List of available backup sets area.
19) Wait until the files have been loaded onto the system and then click **OK & Next**. The recovery of the configuration data is started. The progress of the restore process is displayed.
20) After the message **Restore complete!** appears, the system will automatically reboot. The restoration is completed successfully when the system is ready for use again.

NOTICE: After the restoration the device should be deleted from the RSP server and then to be reconfigured.

25.7 Power Management

Power management automatically switches the communication system to low power mode, depending on the system load. This reduces the energy consumption of the system and thus also contributes to environmental

protection. The time period in which the system switches to low power mode can be set (e.g., at night).

Power management can be enabled only if is the LAN interfaces of the system are in the Ethernet Link Mode **Auto**. In the low power mode, the LAN interfaces of the system automatically switch to the 100 Mbit/s full-duplex mode. The LAN interfaces of the connected infrastructure should also be in the autosense mode.

Operating Modes

- Active Mode

  In active mode, the functions of the communication system are frequently used, and significant data transfers occur between the system and the connected infrastructure.
- Idle Mode

  In idle mode, the functions of the communication system are rarely used, and no significant data transfers occur between the system and the connected infrastructure. When a function is initiated, the system switches from idle mode to active mode.
- Low Power Mode

  Low-power mode has reduced energy requirements compared to the idle mode. The system operates in the 100 Mbit/s full-duplex mode.

It is also possible to operate the system permanently in the Ethernet Link Mode 100 Mbit/s full duplex or 100Mbit/s full duplex.

25.7.1 How to Enable or Disable the Power Management

Prerequisites

The LAN interface of the mainboard, via which the system is connected to the LAN infrastructure, is set to the Ethernet Link Mode **Auto**.

Only if a UC Booster Card is connected: the LAN interface of the UC Booster Card, via which the UC Booster Card is connected to the LAN infrastructure, is set to the Ethernet Link Mode **Auto**.

The LAN interfaces of the connected infrastructure (e.g., IP phones) is set to autosense mode.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.

2) In the navigation tree, click **Wizards** > **Basic Installation**.

3) Click **Edit** to start the **Power Management** wizard.

4) If you want to enable the power management:

a) Select the **Power Management on/off** check box.

b) Under **Start of LowPowerMode** and **End of LowPowerMode**, enter the time span in which the communication system should switch to the low power mode.

5) If you want to disable the power management, clear the **Power Management on/off** check box.

6) Click on **OK & Next**. Your settings are applied.
7) Click on **Finish**.

25.7.2 How to Change the Ethernet Link Mode the LAN Interfaces

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Telephony** > **Network Interfaces** in the navigation tree.
3) Select the Ethernet link mode for the LAN interface of the mainboard:
   a) Click on **Mainboard** > **LAN 2** in the menu tree. The communication system is integrated in the LAN infrastructure via the LAN 2 port.
   b) If you want to enable the power management, select the list item **Auto** from the **Ethernet Link Mode** drop-down list.
   c) If you want to set the system to low power mode permanently, select the list item **100HDX** or **100FDX** from the **Ethernet Link Mode** drop-down list.

      NOTICE:

      Power management cannot be enabled for the Ethernet link modes **100HDX**, **100FDX** and **1000FDX**.

   d) Click on **Apply**.
4) Only if a UC Booster Card is inserted: select the Ethernet Link Mode for the LAN interface of the UC Booster Card:
   a) Click in the menu tree on **Application Board** > **LAN 2** or **LAN 1**, depending on which LAN interface was used to connect the UC Booster Card to the LAN infrastructure (indicated by the check mark in the **Interface Is Active** check box).
   b) If you want to enable the power management, select the list item **Auto** from the **Ethernet Link Mode** drop-down list.
   c) If you want to set the system to low power mode permanently, select the list item **100HDX** or **100FDX** from the **Ethernet Link Mode** drop-down list.

      NOTICE:

      Power management cannot be enabled for the Ethernet link modes **100HDX**, **100FDX** and **1000FDX**.

   d) Click on **Apply**.

25.8 Monitoring and Maintenance of OpenScape Business

OpenScape Business offers different functions for monitoring the current status of the system and for finding and resolving errors.

25.8.1 Checking the Network Connection of OpenScape Business X

The network connection between an OpenScape Business X communication system and the target address can be checked by using an ICMP (Internet Control Message Protocol) request.

Echo request packets can be sent via both the **Ping** and **Traceroute** functions. The corresponding echo reply messages are displayed together with the round-trip times.

The **Traceroute** function sends echo request packets with various incremental TTL (Time-To-Live) values.

25.8.1.1 How to Ping

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **IP Diagnostics** in the navigation tree.
3) Navigate in the menu tree to **IP Routing** > **ICMP Request** > **Ping**.
4) Enter the IP address of the desired target in the **Target Address** field.
5) In the field **Number of Echo Requests to Send**, enter the desired number (default value = 3).
6) Click on **Send**.

   The acknowledgements will then be displayed together with the round trip delays.

25.8.1.2 How to Test the Trace Route

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **IP Diagnostics** in the navigation tree.
3) Navigate in the menu tree to **Mainboard** > **ICMP Request** > **Trace route**.
4) Enter the IP address of the desired target in the **Target Address** field.
5) Enter the desired value (default value = 0) in the **TOS Byte** field.
6) Click on **Send**.

   The acknowledgements will then be displayed together with the round trip delays.

25.8.2 SNMP (Simple Network Management Protocol)

The Simple Network Management Protocol (SNMP) is a network protocol which can be used to monitor and operate networking components (such as routers, servers, switches, printers, PCs) from a central station (management console). The protocol controls communication between the monitored components and the monitoring station.

SNMP describes the structure of data packets that can be sent and the communication procedure. SNMP was designed so that all network-capable devices can be included in monitoring. SNMP-based network management tasks include

- monitoring networking components,
- performing remote control and remote configuration of networking components,
- error detection and notification.

Devices known as "agents" are used for monitoring. These are utilities that run directly on monitored components. These utilities are able to record the status of components, make settings, and trigger actions. SNMP allows the central management console to communicate with the agents over a network.

NOTICE: OpenScape Business supports SNMPv2c, but also responds to SNMPv1 snmpget requests.

Management Information Databases (MIB)

The volume of data that can be administered via SNMP is defined in MIBs (Management Information Base). MIBs are data models that describe the networking components to be administered in an established manner. The MIB of the OpenScape Business X communication systems can be downloaded via the WBM (Service Center).

The communication systems have a separate SNMP agent that allows access to various system data that is stored in its MIB or Management Information Base. The MIB provides basic system information, status information, event-related data, and information on installed hardware (slots) and configured connections (ports).

SNMP supports the central monitoring and administration of networking components, including the communication systems themselves. It is possible to

- address the communication system over the TCP/IP protocol.
- access data over external management applications.
- perform remote maintenance activities.
- visualize the operating status of the communication system.
- transmit service-specific errors (Traps).

Communities

Access to the SNMP data (MIBs) is governed by communities. A distinction is made here between read, write, and Trap communities. Each community has a specific IP address.

To enable read access to SNMP data (MIBs) on a PC, for example, the IP address of this PC must be entered in the list of read communities. To enable

read and write access, the IP address must be entered in the list of write communities.

Trap Communities are used to manage the recipients of error messages (traps).

Traps

When problems occur in a communication system, traps are generated to indicate errors and failures. The following types of traps are available:

- System traps = System errors that require immediate action for recovery.
- Performance Traps = Information on performance problems that do not require corrective action.

Traps are classified by their effects and can be retrieved by an administrator with the **Expert** profile using the WBM. A list of all traps received is displayed with the following information:

Table column	Meaning
VarBind1 (Severity)	Trap effect classes The following entries are possible: Critical: Error Message. This error causes problems. Major: error message. This error could cause problems. Minor: error message. The error has no problematic consequences. Warning: report of a possibly problematic procedure or status, but not an error message. Deleted Information: plain status messages, no error messages. Intermediate status Other traps
VarBind2 (Name)	Trap name
Generic Name	General Description such as Enterprise Specific, for example
Specific Name	Trap type (1 = software, 2 = hardware)
Enterprise	–
Time	Time of error
Index	List number

Trap display is updated every 30 seconds. Traps are sorted in the sequence of occurrence.

Trap details can be displayed by clicking a trap name.

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
Error Class 01 - General Messages				

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
	System Restart	Hard restart (reset) of entire system with current CDB.	None	
FP_EVT_ADM_002	reload of signed slot	reload of signed slot		
FP_EVT_ADM_003	system restart	system restart		
FP_EVT_ADM_010	SNMP System Restart	Hard restart of entire system via SNMP.	None	
FP_EVT_ADM_014	SNMP local DB changes	'On site' changes to the database.	None	
FP_EVT_ADM_015	SNMP remote DB changes	'Remote' changes to the database.	None	
FP_EVT_ADM_016	SNMP APSXF result	APS transfer acknowledgement message via SNMP.	None	
FP_EVT_ADM_017	SNMP authentication fail	Unauthorized access attempt.	Check firewall settings in OpenScape Business/ Manager E (Network ' Firewall).	
FP_EVT_ADM_019	Sensor Alarm	Temperature in OpenScape Business housing is too high.	Check the fan and air supply in the 19' housing. Note the ambient temperature.	
FP_EVT_ADM_020	CDR buffer limit reached	Overflow in the CDR buffer (CDR information).	Check that the interfaces (V.24, LAN), ports and the connection are functioning or read out call data.	
FP_EVT_ADM_024	unauthorized application	Attempted access via an unauthorized application.	Check firewall settings in OpenScape Business/ Manager E (Network ' Firewall).	
FP_EVT_ADM_025	manual switchback from HiPath Manager			
Error Class 02 - License Management Messages				
Error Class 09 - Hardware Module Messages				
FP_EVT_HW_034	loss of frame on (STMD)	loss of frame on (STMD)		
FP_EVT_HW_035	loss of frame off (STMD)	loss of frame off (STMD)		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_HW_036	slip detected on (STMD)	A bit slip has occurred on an ISDN line.	Check the S0 line. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	The problem may be caused by asynchronous internal and external clock rates. Data loss possible/ connection may be terminated.
FP_EVT_HW_039	alarm indication signal error off(TMS2M)	Alarm display: The S2M error has been corrected.	None	
FP_EVT_HW_040	degraded minute error on (TMS2M)	degraded minute error on (TMS2M)		
FP_EVT_HW_041	degraded minute error off (TMS2M)	degraded minute error off (TMS2M)		
FP_EVT_HW_042	no signal error on (TMS2M/STMD)	Alarm display: An S2M error has occurred. No physical connection available.	Check the S2M line and board. If necessary, reload the board or perform a hard restart. If the error persists, set up an ISDN trace.	
FP_EVT_HW_043	no signal error off (TMS2M/STMD)	Alarm display: The S2M error has been corrected.	None	
FP_EVT_HW_046	severely errored seconds error on(TMS2M)	severely errored seconds error on(TMS2M)		
FP_EVT_HW_047	severely errored seconds error of(TMS2M)	severely errored seconds error of(TMS2M)		
FP_EVT_HW_052	clock can be used as ref. (TMS2M/STMD)	clock can be used as ref. (TMS2M/STMD)		
FP_EVT_HW_053	clock can not be used as reference	clock can not be used as reference		
FP_EVT_HW_060	Access power feed error on (SLMO)	Access power feed error on (SLMO)		
FP_EVT_HW_063	ELIC error on (SLMO/ SLMC)	ELIC error on (SLMO/ SLMC)		
FP_EVT_HW_064	ELIC error off (SLMO/ SLMC)	ELIC error off (SLMO/ SLMC)		
FP_EVT_HW_067	OCTAT error on (SLMC)	OCTAT error on (SLMC)		
FP_EVT_HW_096	unknown error from LW	unknown error from LW		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
Error Class 11 - General Messages				
FP_EVT_DEV_041	L1 asynchron on	L1 asynchron on		
FP_EVT_DEV_042	L1 asynchron off	L1 asynchron off		
FP_EVT_DEV_043	Overload error on	Overload error on		
FP_EVT_DEV_044	Overload error off	Overload error off		
FP_EVT_DEV_045	Alive check error on	Alive check error on		
FP_EVT_DEV_046	optiPoint info	optiPoint info		
FP_EVT_DEV_048	Layer 2 error detected	Layer 2 error detected		
FP_EVT_DEV_049	Layer 3 error detected	Layer 3 error detected		
FP_EVT_DEV_052	Other errors	Other errors		
FP_EVT_DEV_057	NO TEI available	NO TEI available		
FP_EVT_DEV_058	Too many L1 errors	Too many layer 1 errors.	Check the lines, terminal, and port. A short circuit may have occurred.	
FP_EVT_DEV_059	Access not configured	Access not configured		
Error Class 16 - Operating System Messages				
FP_EVT_GEN_002	Error in release pool	Error in release pool	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_004	Error in OSF-Send	Error in OSF-Send	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_005	Error in OSF-Timer	Error in OSF-Timer	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_010	RESTARTED: manual Reset	RESTARTED: manual Reset	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_GEN_011	RESTARTED: manual Reload	RESTARTED due to manual Reload	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_012	RESTARTED: Power down	RESTARTED due to Power down	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_013	KDS backup not performed	KDS backup not performed	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_014	RESTARTED: unknown rest. HW ind. missmatch	RESTARTED due to unknown rest. HW ind. missmatch	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_015	general error logging	general error logging	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_020	CSTA: length out of range	CSTA: length out of range	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_024	idle arrived after restart	idle arrived after restart	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	
FP_EVT_GEN_030	exceed. of CSTA mon. pts	exceed. of CSTA mon. pts	Set up a trace using information from BLS (Back Level Support). Create a stack dump. Save a snapshot.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
Error Class 19 - Network Services Messages				
FP_EVT_NWS_011	SNTP-Client at PCS can't be activated	SNTP-Client at PCS can't be activated		
Error Class 20 - Call Processing Messages				
FP_EVT_CP_002	RS232: DSR not Ready	The RS232/V.24 interface is out of order.	Check the interface, the line, and the application.	
FP_EVT_CP_013	not connected ways	The maximum number of connection paths permitted has been exceeded.	Use the project planning tool to test the system configuration. Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
Error Class 21 - Device Handler Messages				
FP_EVT_DH_004	Port out of service	Port out of service		
FP_EVT_DH_005	Port in service	Port in service		
FP_EVT_DH_016	Name in S0/S2M msg discard	Name in S0/S2M msg discard		
FP_EVT_DH_017	msg to long L3S int->ext	msg to long L3S int->ext		
FP_EVT_DH_018	msg to long L3S ext->int	msg to long L3S ext->int		
FP_EVT_DH_022	Auto PRI detec DMS250 prot	Auto PRI detec DMS250 prot		
FP_EVT_DH_023	Auto PRI detect NI2 prot		Auto PRI detect NI2 prot	I
FP_EVT_DH_024	Auto PRI detect 4ESS prot		Auto PRI detect 4ESS prot	
FP_EVT_DH_026	key module overflow	key module overflow		
FP_EVT_DH_027	B-chan limit reached	B-chan limit reached		
Error Class 23 - Device Handler Messages				
FP_EVT_NW_060	system hold, no buffer available	System hold, no more free buffer available.	Set up a trace using information from BLS. Create a stack dump. Save a snapshot.	
Error Class 26 - Board Administration Messages				
FP_EVT_PR_001	card out of service	The specified board is out of order.	None	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
FP_EVT_PR_003	other card type than old card type	Incompatible board type. The slot is already pre-assigned with a different board type.	Replace the board or use Assistant T to delete the preassigned board type so that the new board is recognized.	
FP_EVT_PR_004	card in service	The specified board is operational.	None	
FP_EVT_PR_005	error during database read	error during database read		
Error Class 28 - Recovery Messages				
FP_EVT_RC_008	Missing APS in EventLog B	Missing APS in EventLog B	None	The current APS version is entered when the event log B memory is copied. This facilitates analysis.
Error Class 30 - Board Software Messages				
FP_EVT_LW_095	no USBS connection to system	no USBS connection to system		
Messages Concerning Resource Manager				
FP_EVT_RM_001	Resource Manager error configuration	Resource Manager error configuration		
Messages Concerning UPM				
FP_EVT_UPM_010	UPM: restarted	UPM: restarted		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_DLSC_BOOTSTRAP_OK	DLS client successfully bootstraped.	DLS client successfully bootstraped.		
MSG_STRC_STOP	Secure trace stopped.	Secure trace stopped.		
MSG_STRC_START	Secure trace started for protocols.	Secure traces have been activated by user for the mentioned protocols.		
MSG_SPE_CERT_MISSING	SPE certificate missing.	No SPE certificate installed.	Import SPE certificate plus private key (PKCS#12 file).	
MSG_SPE_CERT_AVAIL	SPE certificate available.	SPE certificate is now available.		
MSG_SPE_CERT_UPDATED	SPE certificate has been updated successfully.	SPE certificate has been updated successfully.		
MSG_SPE_CERT_EXPIRED	SPE certificate expired.	Validity period of installed SPE certificate is passed.	Install a new valid certificate.	

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_SPE_CRL_EXPIRED	SPE CRL for a specific CA has been expired.	CDP inaccessible or retrieved CRL is expired.	Import a SPE CA certificate with valid CRLs configured in CDP.	
MSG_SPE_CRL_UPDATED	SPE CRL for CA has been updated successfully.	SPE CRL for CA has been updated successfully.		
MSG_SPE_ALL_CRLS_UPTODATE	All SPE CRLs are up to date again.	All SPE CRLs are up to date again.		
MSG_MIKEY_REBOOT	Mikey Stack: assertion failed.	Mikey Stack: assertion failed.		
MSG_IPSEC_REBOOT	Fatal error in IPSec stack.	Fatal error in IPSec stack.		
MSG_CAT_H323_REBOOT		Reboot with H.323		
MSG_CAT_HSA_REBOOT		Reboot with HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 up/down		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				
MSG_ADMIN_REBOOT		Reboot with WBM/ CLI-Admin, software upgrade or data restore		
MSG_SYSTEM_REBOOT		Automatic reboot, for example with Garbage Collection		
MSG_EXCEPTION_REBOOT		Reboot with SW exception		
MSG_GW_OBJ_MEMORY_EXHAUSTED		Out of memory		
MSG_TLS_POOL_SIZE_EXCEEDED		No more internal pools		
MSG_OAM_RAM_THRESHOLD_REACHED		RAM limit reached		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		DRAM limit reached		
MSG_OAM_THRESHOLD_REACHED		Limit reached, for example, for flash memory or IP pools		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Temperature limit reached (too hot)		
MSG_HACKER_ON_SNMP_PORT_TRAP		Unauthorized access to SNMP port		
MSG_DVMGR_LAYER2_SERVICE_TRAP		B channel up/down		

SNMP Code	Event Log Entry	Meaning	Required Measures	Note
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	More than 2 call Legs: not supported! CSID: %x/%x	No more than two call Legs per session are permitted. This has caused the software to become unstable. The necessary reboot is executed.		
MSG_SSM_SESSION_CREATION_FAILED	Session creation failed	Signalling is no longer possible because a session could not be created. The necessary reboot is executed. An SNMP trap is generated.		
MSG_IPNCV_STARTUP_ERROR	IPNCV Startup: Creating IPNCV Manager failed	IPNCV could not be started. An SNMP trap is generated.	Create a TR/MR	
MSG_IPNCV_STARTUP_SHUTDOWN	IPNCV start/stop: IPNCV Manager created successfully or IPNCV start/stop: Shutdown of IPNCV Manager successfully	IPNCV was started or stopped successfully.An SNMP trap is generated		
MSG_IPNCV_INTERNAL_ERROR	Internal IPNCV error: %s	Software error: invalid internal data found.An SNMP trap will be generated with the profile IPNCV-Detailed.		
MSG_IPNCV_MEMORY_ERROR	IPNCV Memory: %s	Memory overflow: an SNMP trap is generated.	Restart the gateway. Create a TR/MR.	
MSG_IPNCV_SIGNALING_ERROR	IPNCV Signaling Error: %s	Software error: invalid internal data found.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR : Alive : ip connection %d.%d.%d.%d lost	CAR: Alive: IP connection lost.		
MSG_LIC_DATA_ACCEPTED		License data accepted		
MSG_LIC_DATA_CORRUPTED		License data incomplete		
MSG_LIC_DATA_NOT_ACCEPTED		License data accepted		
MSG_SPE_CERT_MISSING	No SPE certificate installed!	SPE certificate missing.	Install SPE certificate.	

NOTICE: There are SNMP events not documented in this guide.

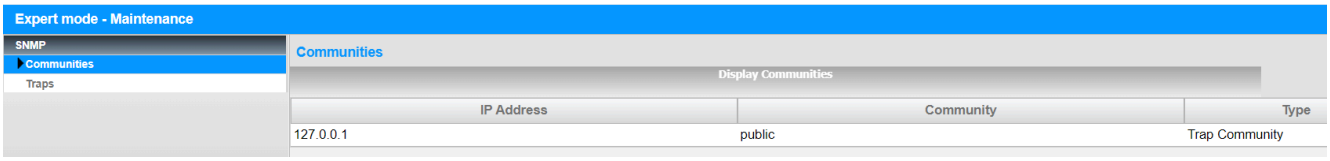
25.8.2.1 How to Display all Communities

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.
3) Click on **SNMP** > **Communities** in the menu tree. A list of all communities is displayed with the associated data (IP address, community, type).



25.8.2.2 How to Add a Community

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.
3) Select the desired community.
   - If you want to add a Read Community, click **SNMP** > **Communities** > **Read Communities** in the menu tree. Click on the **Add Read Community** tab.
   - If you want to add a Write Community, click **SNMP** > **Communities** > **Write Communities** in the menu tree. Click on the **Add Write Community** tab.
   - If you want to add a Trap Community, click **SNMP** > **Communities** > **Trap Communities** in the menu tree. Click on the **Add Trap Community** tab.
4) Enter the IP address of the new community in the **IP Address** field.
5) Enter the name of the new community in the **Community** field.
6) Click on **Apply** followed by **OK**.

25.8.2.3 How to Edit a Community

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.

3) Navigate in the menu tree under **SNMP** > **Communities** > **...** down to the desired community.
4) Click on the **Edit Community** tab.
5) Edit the community.
6) Click on **Apply** followed by **OK**.

25.8.2.4 How to Delete a Community

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.
3) Navigate in the menu tree under **SNMP** > **Communities** > **...** down to the desired community.
4) Click on the **Delete Community** tab.
5) Click on **Delete** followed by **OK**.

25.8.2.5 How to Display Traps

Prerequisites

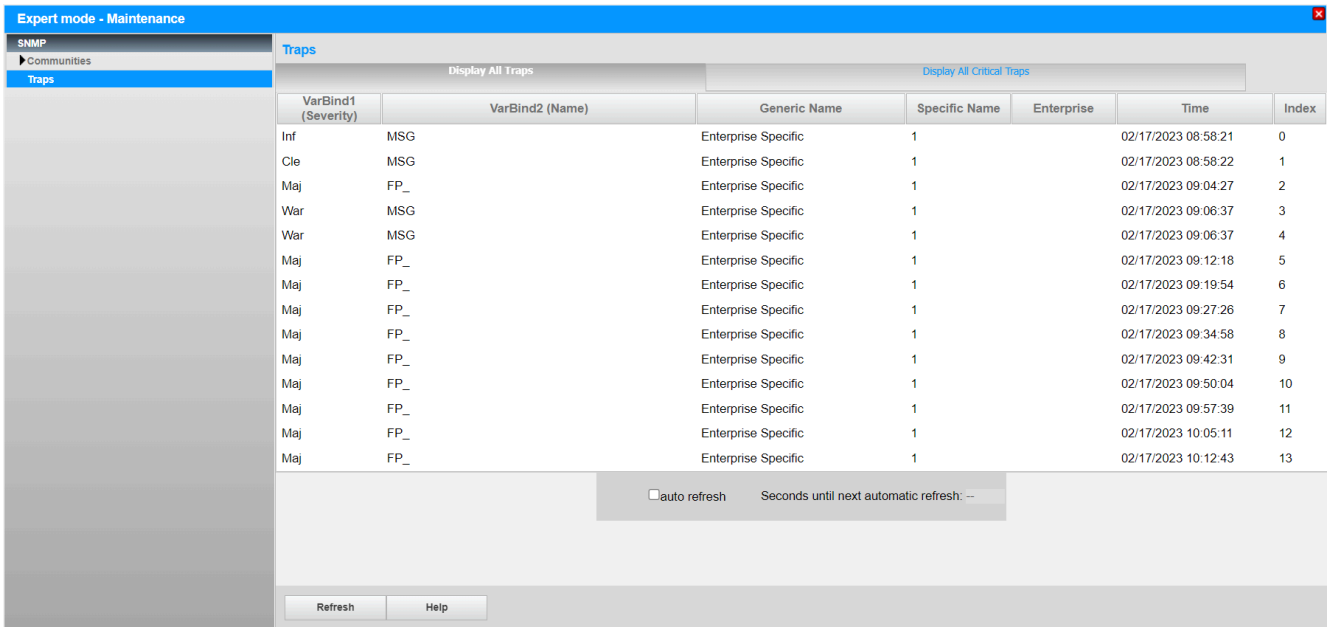
You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.
3) Click on **SNMP** > **Traps** in the menu tree.

4) Select one of the following options:

- If you want a list of all traps to be displayed, click the **Display All Traps** tab.



- If you want a list of all critical traps to be displayed, click the **Display All Critical Traps** tab.

25.8.2.6 How to Display Details of a Trap

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **SNMP** in the navigation tree.
3) Click on **SNMP** > **Traps** in the menu tree.
4) Click on the **Display All Traps** tab. A list of all traps is displayed with the associated data.
5) Click on the name of the desired trap. The details of that trap will be displayed.
6) Click on the **Display All Traps** tab to open the list of all traps once more.

25.8.3 Manual Actions

Many different logs (diagnostics data and diagnosis logs) can be loaded via manual actions.

Administrators with the **Advanced** profile can load diagnostic data (diagnosis logs) by using the **Trace** wizard.

Administrators with the **Expert** profile can load diagnostic data (diagnosis logs) in **Expert mode**.

The following logs can be loaded:

Protocol	Explanation	Application case
Trace log	Standard trace file, if trace profiles have been activated. A selection can be made between the following options: • **Complete Trace Log**: The full set of existing system trace log files is downloaded. • **Log from Today**: The system trace log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The system trace log files of the selected time period are downloaded.	No special application
Event Log	Actions/events of the communication system (Reset, On/Off, etc.)	No special application
Admin log (also called admin protocol)	Messages about administration processes at the communication system (login attempts, etc.)	No special application
License Protocols	Messages about the communication system components that require licenses	Problems with licensing (the license file cannot be activated, and so on)
Customer Trace	Messages for the customer trace are provided in a more detailed format than in the trace log, for example (remote login, ITSP login, etc.).	Problems with the ITSP (Internet Telephony Service Provider) connection or the remote login
Framework Protocol	WBM messages	Problems with licensing, backup, restore or with the WBM
Diagnosis Log	Diagnosis logs of the communication system (FP/LDH)	System crash or uncontrolled shutdown of the communication system

Protocol	Explanation	Application case
UC Suite Logs	Messages of the UC Suite of the communication system (UC Suite, CSP and MEB logs) A selection can be made between the following options: • **Complete Trace Log**: All existing UC Suite, CSP and MEB log files are downloaded. • **Log from Today**: The UC Suite, CSP and MEB log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The UC Suite, CSP and MEB log files of the selected time period are downloaded. All log files are archived together in a compressed file. The following file naming conventions apply to the OpenScape Business logs: UC Suite log files = `vs_yyyy_mm_dd.log`, CSP log files = `csptrace_yyyy_mm_dd.log`, MEB log files = `mebtrace_yyyy_mm_dd.log`. ***INFO***: diagnostic data can be downloaded only when operating with the UC Booster Card OCAB. When using the OpenScape UC Business Booster Server, diagnostic data must be downloaded from the server itself.	Problems with the UC Suite and/or the client (myPortal for Desktop, myAttendant, etc.)
Application Protocols	Messages of the application side of the communication system (for example, CSP protocols) An administrator with the **Expert** profile can select between the following options in **Expert Mode**: • **Complete Trace Log**: All existing log files are downloaded • **Log from Today**: The log files of the current day (as of 00:00 hours) are downloaded. • **Own Selection**: **From:** XXX **To:** YYY: The log files of the selected time period are downloaded. All log files are archived together in a compressed file.	Problems with the application side of the communication system
System Diagnosis Logs	Diagnosis logs of the communication system	No special application
PPP Logs	Messages for the Point-to-Point Protocol	Problems with Dial-In or Dial-Out connections
CoreLog Protocol	CoreLogs are created for resets, etc. (e.g., memory dumps at a PC).	System crash or uncontrolled shutdown of OpenScape Business

After the desired logs have been selected, a compressed file is created and stored in a specified directory.

25.8.3.1 How to Download Diagnostics Data / Diagnosis Logs

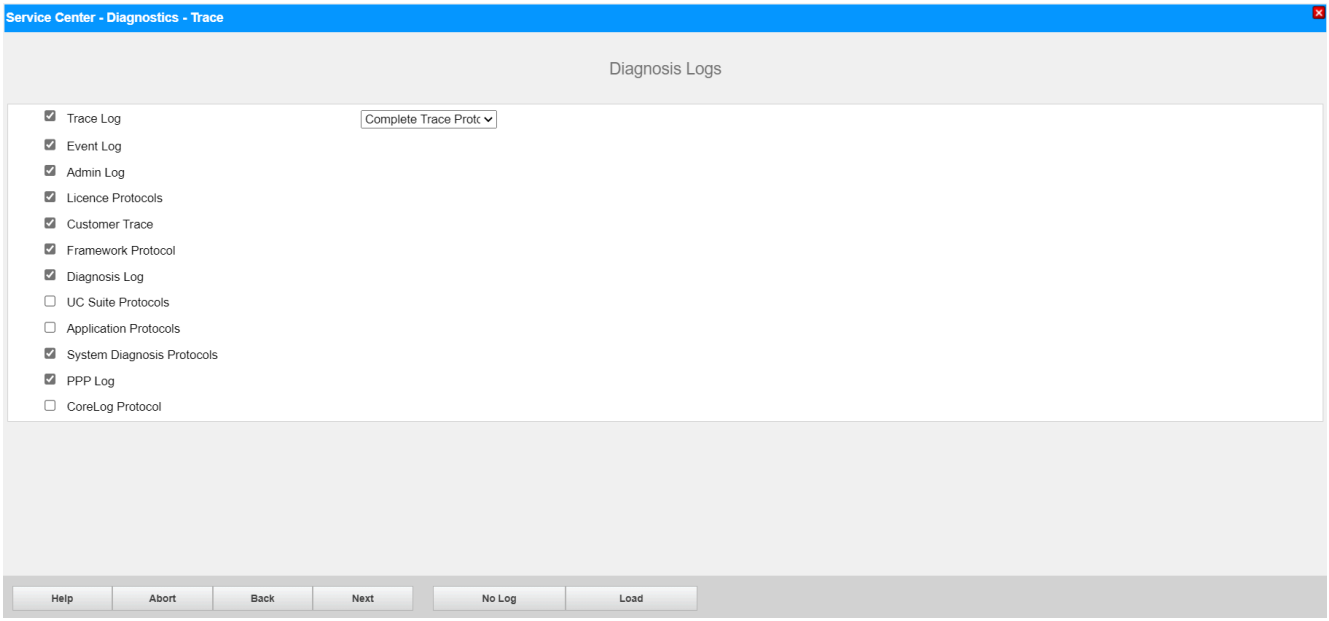
The **Trace** wizard can be used to download diagnostics data (diagnosis logs) for the communication systems.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree.
3) Click on **Diagnosis Logs**.



4) Select the check boxes of the logs you want to download. Clear the check boxes of the logs you do not want to download.
5) Click on **Load** followed by **OK**. The File Download window appears.
6) Save the file in the desired directory. Then close the window that confirms the download of the file.
7) Click on **Next** followed by **Finish**.

25.8.4 Traces

Traces can be used to record the execution of individual program steps and their results during the execution of a program. In combination with further diagnostics data, an incorrectly executing program can be traced back to the source of the error. The individual traces to be recorded and their respective levels of detail are configured via the trace profiles and trace components.

INFO: Activating traces can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

The console trace, in particular, requires substantial system resources and thus has an adverse effect on the performance of the communication system.

Networking

In order to diagnose networked communication systems, the trace data of each individual node must be collected separately. It is not possible to acquire the trace data of networked communication systems centrally.

Trace Format Configuration

The Trace Format Configuration function can be used by an administrator with the **Expert** profile to define which header data is to be included in the trace output and how the trace data is to be formatted.

Header data for the trace output (all options are activated in the default setting):

- Global Trace Header Format Settings

  If this option is enabled, the options for the following header data can be activated or deactivated.
- Subsystem ID
- Task Name
- Task ID
- Time
- Module Name
- Line Number

Formatting the Trace Data

- Full formatting with parameter expansion (default) = large data volume, normal trace performance. Default setting
- Limited formatting (message types binary, special X-Tracer format) = medium data volume, fast trace performance.
- Limited formatting (expansion of basic data types only) = low data volume, very trace performance.
- Performance optimized trace without parameter expansion = very low data volume, extremely fast trace performance.

INFO:

Note that adding more trace header data and extensive trace data formatting will decrease the overall trace performance.

Trace output interfaces

This function enables an administrator with the **Expert** profile to define the interfaces for the trace output. It is possible to either enable the file trace or trace via LAN or to disable both interfaces.

Trace output interface	Explanation	Default setting
File Trace	**Switch File Trace On** Trace messages are entered into a log file in the communication system. The following settings apply when the option is enabled: **Max. Trace Quota (kByte)**: Indicates the maximum size of the trace memory **Policy to handle reach of max. quota**. You can choose between **Wrap Around (delete oldest file)** and **Stop temporarily the file trace**. **Time between creation of new trace files (sec):** 900 **Time period for which trace files are available:** The actual time period is specified.	Enabled
Trace via LAN	**Switch Trace via LAN On** Trace messages are transmitted via the LAN interface. The following setting applies when the option is enabled: **Timer value** = 25 sec. (delay period until data is transmitted.)	Not activated

Trace log

If the trace output interface Switch File Trace On is enabled, the resulting log files can be transferred by an administrator with the **Expert** profile to a PC or deleted.

Digital Loopback

Digital loopbacks are used to test the B channels of S_0, S_{2M} and T1 interfaces of any existing boards. Digital loopbacks should only be activated if requested by the service provider.

They can only be configured using E Manager.

Event Viewer / Customer Trace Log

The **Event Viewer** wizard can be used by an administrator with the **Advanced** profile to start the event display (customer trace) In addition, the customer trace log file can be copied to a PC or deleted.

The following functions, which can be started using the wizard, are described here:

- How to Display or Edit Event Viewer and Customer Trace Logs
- How to Download or Open the Event Viewer Log / Customer Trace Log
- How to Clear the Event Viewer Log / Customer Trace Log

Administrators with the **Expert** profile can start displaying the customer trace log file in **Expert mode**. In addition, the customer trace log file can be copied to a PC or deleted.

M5T Trace Components

This function is used to monitor the SIP stack by an administrator with the **Expert** profile. For each M5T trace component, the level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 4 = maximum level of detail).

Secure Trace

This function is used by an administrator with the **Expert** profile to record encrypted VoIP payload and signaling data streams.

If the Signaling and Payload Encryption (SPE) feature has been enabled, the VoIP payload and signaling data streams from and to the communication system and between IP phones will be encrypted.

To ensure that errors are properly analyzed, additional trace information (**Secure Trace**) can be transmitted in the LAN for a limited period of time. In this case, asymmetrically encrypted secure trace files are generated, which can only be decrypted and analyzed by Development.

The following security features have been implemented to restrict the use of the secure trace function:

- A service technician must import a so-called public key (certificate) into the relevant communication system. The certificate is part of an X.509 file and is required to generate a secure trace. The X.509 file is provided by Development. The included certificate is valid for a maximum of one month.
- A special password (passphrase) must be entered to start and stop the secure trace. This password is known only to the customer.

Thus, the certificate is the key of the service technician and the password (passphrase) is the key of the customer. Both keys are required to activate the secure trace function.

Process for generating a secure trace:

1) A service technician finds a problem in the customer's LAN. Together with Development, the service technician recognizes the need to generate a secure trace.

2) The customer is notified accordingly and must confirm that he has been notified. The customer then issues an order for the creation of a secure trace, specifying the date and time when monitoring should start and end.

3) A developer creates a key pair consisting of the public key and the private key. This key pair can only be used to create a single secure trace. The certificates are used in the following manner

   - The certificate with the private key is strictly confidential and can only be used by authorized developers.

     The private key is required to decrypt the secure trace files.
   - The certificate with the public key is passed to the service technician in the form an X.509 file in PEM or binary format.

     This certificate must be imported into the relevant communication system to be able to generate a secure trace.

4) The service technician notifies the customer that the generation of the secure trace is to start soon. The customer, in turn, must notify all affected parties.

NOTICE: The live recording of calls and connection data is a criminal offence, unless the affected parties have been notified in advance.

5) The service technician imports the certificate with the public key into the relevant communication system.
6) The customer starts the secure trace by entering the password (passphrase). The secure trace files are generated.

   Start and stop of the secure trace are logged by the communication system.
7) Upon completion of secure trace generation, the customer is notified that all secure trace activities have been stopped. The service technician removes the certificate from the communication system.
8) The secure trace files are made available to Development.
9) A developer decrypts the secure trace files using the private key and then analyzes the decrypted data.

NOTICE: Once the analysis has been completed, all relevant data must be destroyed in a secure manner. This includes the destruction of the private key so that any potential unauthorized copy of the secure trace files can no longer be decrypted.

H.323 Stack Trace

This function can be used by an administrator with the **Expert** profile to set the H.323 Stack Trace Configuration. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 4 = maximum level of detail). The following settings can be selected for the H.323 stack trace output:

Trace output interface	Explanation	Default setting
Console Trace	**Switch Console Trace On** H.323 Stack Trace messages are output on the console.	Not activated
File Trace	**Switch File Trace On** H.323 Stack Trace messages are written to a log file. The following settings apply when the option is enabled: Max. size of the trace buffer = 50000 bytes (amount of data stored in the buffer.) Max. size of the trace file = 1000000 bytes (maximum size of the log file.) Trace Timer = 60 sec. (delay period until data is written to the log file.)	Not activated

By activating and/or deactivating H.323 modules, you can define for which components of the H.323 stack trace the process and status information is

to be recorded. The status of each H.323 module is indicated by the color of the associated bullet point (green = H.323 module active, red = H.323 module inactive).

The H.323 Stack Trace log can be transmitted to a PC or deleted.

License Component Trace

This function is used by an administrator with the Expert profile to monitor the system-internal license agent (Customer License Agent, CLA). The level of detail for the trace can be defined via trace levels (low = lowest level of detail (default), standard = medium level of detail, all = maximum level of detail).

By default, the license component trace is enabled (trace level = low).

Changing the trace level can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

Trace Profiles

Trace profiles define what data is to be recorded and at what level of detail. Trace components are assigned to a trace profile. This allows you to specify for which system components the process and status information should be logged by the trace profile.

Predefined trace profiles are provided for all standard scenarios. In addition, an administrator with the **Expert** profile can also create his or her own profiles. When you start a trace profile, logging is activated via this profile. When you stop the profile, logging is deactivated.

- Administrators with the **Advanced** profile can start and/or stop trace profiles by using the **Trace** wizard. The status of every trace profile is indicated by the color of the associated list item (green = trace profile active, red = trace profile not active). **Start/Stop** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

  Load Trace is used to transfer the generated log files to a PC or open them.

  Delete Trace is used to delete the generated log files.

  The following functions, which can be started using the wizard, are described here:

  – How to Download a System Trace Log File
  – How to Delete a System Trace Log File
  – How to Display all Trace Profiles
  – How to Start or Stop a Trace Profile
  – How to Download Diagnostics Data / Diagnosis Logs
- Administrators with the **Expert** profile can collectively stop all trace profiles and selectively start and/or stop individual trace profiles in **Expert mode**.

  In the menu tree display, the color of the list item indicates the status of the trace profile (green = trace profile is activated, red = trace profile is not activated). **Start/Stop Trace Profile** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

  By selecting **Display Trace Profile** you can view the details of the desired trace profile: This includes the profile name, details about write protection

and the status of the profile, as well as information on when, i.e., for which problems, this trace profile should be used. In addition, you can see which trace components belong to the trace profile.

Trace Profile	Application case
Actors / Sensors / Door Opener	No information is currently available!
Basic	No information is currently available!
Calls_with_Analog_Subscriber_Trunks	No information is currently available!
Calls_with_ISDN_Subscriber_Trunks	No information is currently available!
Calls_with_System_Device_HFA	No information is currently available!
Calls_with_System_Device_Upn	No information is currently available!
CDR_Charging_data	No information is currently available!
CMI	No information is currently available!
CSTA_application	No information is currently available!
Display_problems	No information is currently available!
Gateway_Stream_detailed	No information is currently available!
Gateway_Stream_overview	No information is currently available!
IP_Interfaces	No information is currently available!
License_problem	No information is currently available!
Network_Call_Routing_LCR	No information is currently available!
Peripheral_cards	No information is currently available!
RAS_or_Internal_access	No information is currently available!
Resources_MOH_Conferencing	No information is currently available!
SIP_Interconnection_Subscriber_ITSP	No information is currently available!
SIP_Registration	No information is currently available!
Smart_VM	No information is currently available!
UC_Smart	No information is currently available!
Voice_fax_connection	No information is currently available!
VPN	No information is currently available!
Web_based_Assistant_Expert_Mode	No information is currently available!

Trace Components

Trace components can be used to record the process and status information of individual components of the communication system.

All trace components can be stopped together and started or stopped individually by an administrator with the **Expert** profile. Starting and stopping a trace component activates and deactivates the recording. The level of detail for the trace can be defined via trace levels (0 = lowest level of detail to 9 = maximum level of detail).

The color of the list item displayed in the menu tree indicates the status of the trace component (green = trace component activated, red = trace component

not activated). **Start/Stop Trace Component** can be used to enable or start an inactive trace component (red bullet point) and to disable or stop an active trace component (green bullet point).

A Trace Component display shows the subsystem name, the trace component index, the set trace level, the status information and whether or not the trace component is currently active. If a trace component needs to be edited, apart from changing the trace level, the trace component can also be started or stopped.

25.8.4.1 How to Download a System Trace Log File

The **Trace** wizard can be used to download system trace log files.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree.
3) Click on **Diagnosis Logs**.
4) Click on **No Log** to clear the check boxes of all logs.
5) Enable the **Trace Log** check box.
6) Select one of the following options:
   - If you want to download the entire system trace log, select **Complete Trace Log** in the drop-down list.
   - If you want to download the system trace log for today, select **Log from Today** in the drop-down list.
   - If you want to download the system trace log for a specific time period, select **Own Selection** in the drop-down list. Then, select the beginning and end of the desired time period in the drop-down lists **From:** and **To:**.
7) Click on **Load** followed by **OK**. The File Download window appears.
8) Save the file in the desired directory. Then close the window that confirms the download of the file.
9) Click on **Next** followed by **Finish**.

25.8.4.2 How to Delete a System Trace Log File

The **Trace** wizard can be used to delete system trace log files.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree.
3) Click on **Delete Trace** followed by **OK**.
4) Click on **Next** followed by **Finish**.

25.8.4.3 How to Set Trace Settings to Default Values

The **Trace** wizard can be used to set system trace log files to the default state.

Prerequisites

You are logged on to the WBM with the **Advanced** or **Expert** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree.
3) Click the **Default Trace Settings** button followed by **OK** in the next pop up message which notifies you that the action is completed successfully.
4) Click on **Next** followed by **Finish**.

NOTICE: Extended tracing increases the general system load and it should not be permanently active. Trace settings should be set back to default by clicking **Default Trace Settings button** as soon as required traces have been successfully created**.**

NOTICE: If extended trace settings are active, you will be notified about this on the home page of the WBM in the **Notifications** area. A direct link to the trace settings of the Service Center is also available.

25.8.4.4 How to Display all Trace Profiles

The **Trace** wizard can be used to obtain information on the status of all trace profiles.

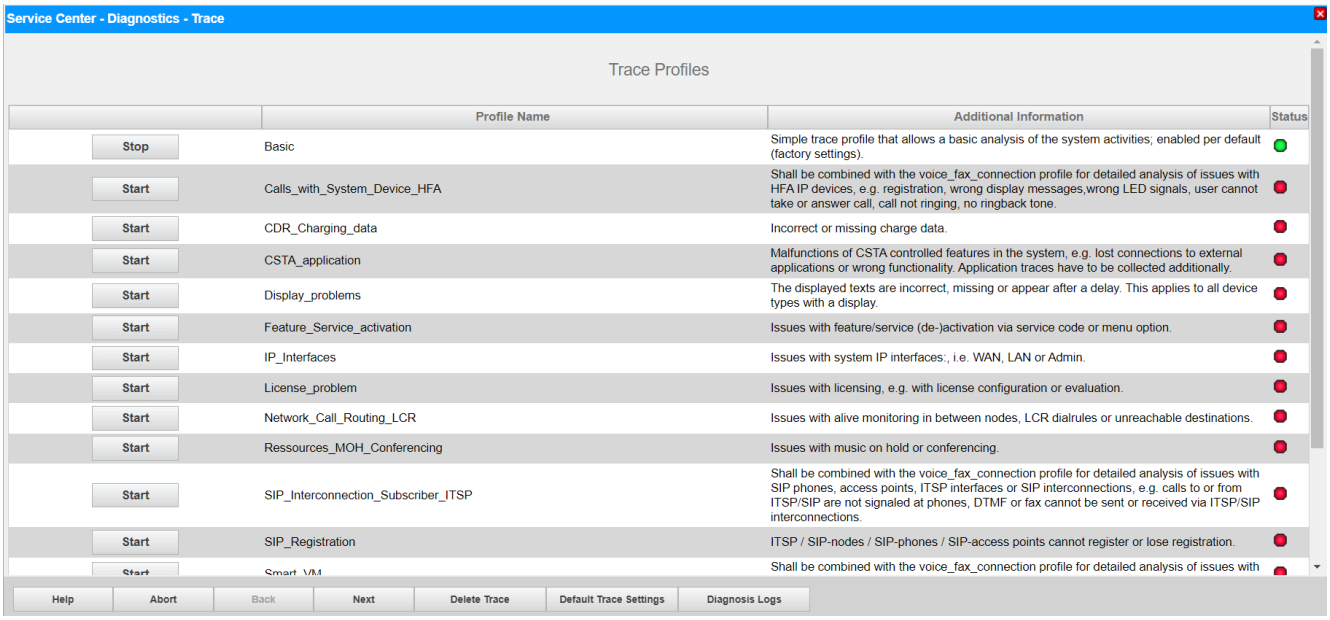
Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) Click **Diagnostics** > **Trace** in the navigation tree. A list of all trace profiles appears, showing which trace profiles are started and which are not started.



3) Click on **Next** followed by **Finish**.

25.8.4.5 How to Start or Stop a Trace Profile

The **Trace** wizard can be used to start and stop trace profiles.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree. A list of all trace profiles appears. A red bullet point indicates the trace profiles that can be started. A green bullet point indicates the trace profiles that can be stopped.
3) Select one of the following options:
   - If you want to start a trace profile, click **Start**. The color of the list item that shows the status of the associated trace profile changes from red to green.

     NOTICE: Started trace profiles can have a negative impact on system performance. Consequently, after you finish your diagnostic activities, make sure that you stop all trace profiles, except for the **Default** trace profile. The **Default** trace profile must remain active.

   - If you want to stop a trace profile, click **Stop**. The color of the list item that shows the status of the associated trace profile changes from green to red.
4) Click on **Next** followed by **Finish**.

25.8.4.6 How to Display or Edit the Trace Format Configuration

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the trace format configuration has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Format Configuration** in the menu tree. The current settings of the trace format configuration are displayed.
4) Change the desired settings if required.
5) Click on **Apply** followed by **OK**.

25.8.4.7 How to Display or Edit the Trace Output Interfaces

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the trace output interfaces has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Output Interfaces** in the menu tree. The Simple Network Management Protocol (SNMP) is a network protocol which can be used to monitor and operate networking components (such as routers, servers, switches, printers, computers) from a central station (management console).
4) Change the desired settings if required.
5) Click on **Apply** followed by **OK**.

25.8.4.8 How to Display or Edit Event Viewer and Customer Trace Logs

The **Event Viewer** wizard can be used to start the event display (customer trace) and to edit the Refresh settings.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Event Viewer** in the navigation tree.
3) Click on the **Display** tab.

4) Select the desired setting.
   - If you want the log to automatically refresh, select the **auto refresh** check box.
   - If you do not want the log to automatically refresh, clear the **auto refresh** check box.
5) If required, click **Refresh** to manually refresh the Customer Trace log.
6) Click on **Finish**.

25.8.4.9 How to Download or Open the Event Viewer Log / Customer Trace Log

The **Event Viewer** wizard can be used to open the customer trace log file or to transfer it to a PC.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Event Viewer** in the navigation tree.
3) Click on the **Load via HTTP** tab.
4) Click on **Load** followed by **OK**. The File Download window appears.
5) Select one of the following options:
   - If you want to download the log file, click **Save As**. Save the file in the desired directory and then close the window that confirms the download of the file.
   - If you want to open the log file, click **Open**. The contents of the compressed log file is then displayed.
6) Click on **Finish**.

25.8.4.10 How to Clear the Event Viewer Log / Customer Trace Log

The **Event Viewer** wizard can be used to delete the customer trace log file.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Event Viewer** in the navigation tree.
3) Click on the **Clear Event Log** tab.
4) Click on **Delete Log** followed by **OK**.
5) Click on **Finish**.

25.8.4.11 How to Display M5T Trace Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **M5T Trace Components** in the menu tree. A list of all M5T trace components is displayed with the current settings. In addition, the names of all M5T trace components are displayed in the menu tree. The bullet point color indicates the status of each individual M5T trace component.

25.8.4.12 How to Start or Stop an M5T Trace Component

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to start or stop a M5T trace component has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **M5T Trace Components** in the menu tree. The names of all M5T trace components are displayed in the menu tree. A red bullet point indicates the M5T trace components that can be started. A green bullet point indicates the M5T trace components that can be stopped.
4) Click on the desired M5T trace component in the menu tree.
5) Click on the **Start/Stop Trace Component** tab.
6) Select one of the following options:
   - To start an M5T trace component, click **Start** and then **OK**.
   - To stop an M5T trace component, click **Stop** and then **OK**.

25.8.4.13 How to Edit M5T Trace Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the M5T trace component has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **M5T Trace Components** in the menu tree. A list of all M5T trace components is displayed with the current settings.

4) Change the desired settings.
5) Click on **Apply** followed by **OK**.

25.8.4.14 How to Start or Stop the Secure Trace

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Secure Trace** in the menu tree.
4) Click on the **Start/Stop Secure Trace** tab.
5) Select one of the following options:
   - If you want to test the secure trace, proceed as follows:

     Enter the password for the secure trace in the **Secure Trace Activation Passphrase** field.

     Enter the time in minutes during which the secure trace is to be active in the **Duration of Secure Trace (Mins.)** field.

     Enable the checkboxes of the protocols for which the secure trace should be created. Clear the checkboxes of the protocols for which the secure trace should not be created.

     Click on **Start Secure Trace** followed by **OK**.
   - To stop the secure trace, click **Stop Secure Trace** followed by **OK**.

25.8.4.15 How to Check the Secure Trace Status

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Secure Trace** in the menu tree.
4) Click on the **Secure Trace State** tab. The current status of the secure trace is displayed.

25.8.4.16 How to Change the Secure Trace Password

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Secure Trace** in the menu tree.
4) Click on the **Change Secure Trace Passphrase** tab.
5) Enter the current password for the secure trace in the **Current Passphrase** field.
6) Enter the new password (5 characters min., 12 characters max.) for the secure trace in the **New Passphrase** and **Confirm New Passphrase** fields.
7) Click on **Apply**.

25.8.4.17 How to Import the Certificate for the Secure Trace from an X.509 File

Prerequisites

An X.509 file in PEM or binary format is available.

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Secure Trace** in the menu tree.
4) Click on the **Import X.509 file for Secure Trace** tab.
5) Click on **Browse** to select the desired X.509 file.
6) Click on **Open**.
7) Click on **Import Certificate from File**.

25.8.4.18 How to Display or Edit the H.323 Stack Trace Configuration

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the H.323 stack trace configuration has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **H.323 Stack Trace** in the menu tree.
4) Click on the **Edit H.323 Stack Trace Configuration** tab. The current settings for the H.323 stack trace configuration are displayed.
5) Change the desired settings if required.
6) Click on **Apply** followed by **OK**.

25.8.4.19 How to Edit H.323 Modules

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the H.323 modules has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **H.323 Stack Trace** in the menu tree.
4) Click on the **Edit All H.323 Modules** tab.
5) Select the desired setting for **Trace On**:
   - If you want to enable the trace for specific H.323 modules, select the check boxes for the desired H.323 modules. Disable the checkboxes of the H.323 modules for which the trace is to be deactivated.
   - If you want to disable the trace for all H.323 modules, click **None**.
6) Click on **Apply** followed by **OK**.

25.8.4.20 How to Download or Open the H.323 Stack Trace Log

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **H.323 Stack Trace** in the menu tree.
4) Click on the **Load H.323 Trace Log via HTTP** tab.
5) Click on **Load** followed by **OK**. The File Download window appears.
6) Select one of the following options:
   - If you want to save the H.323 stack trace log file, click **Save As**. Save the file in the desired directory and then close the window that confirms the download of the file.
   - To open the H.323 stack trace log file, click **Open**. The file is then displayed in the text editor.

25.8.4.21 How to Clear the H.323 Trace Log

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **H.323 Stack Trace** in the menu tree.
4) Click on the **Clear H.323 Trace Log** tab.
5) Click on **Delete Log** followed by **OK**.

25.8.4.22 How to Edit the License Component Trace

Prerequisites

You are logged into the WBM with the **Expert** profile.

A request to edit the license component trace has been submitted by the responsible Service Support.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **License Component** > **CLA** in the menu tree.
4) Select one of the following options:
   - If you want to stop the license component trace, select the item **Off** in the **Trace Level** drop-down list.
   - If you want a low level of detail for the trace recording, select the item **Low** in the **Trace Level** drop-down list.
   - If you want a medium level of detail for the trace recording, select the item **Standard** in the **Trace Level** drop-down list.
   - If you want a high level of detail for the trace recording, select the item **All** in the **Trace Level** drop-down list.
5) Click on **Apply**.

25.8.4.23 How to Display Details of a Trace Profile

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Profiles** in the menu tree. A list of all trace profiles appears. In addition, the names of all trace profiles are displayed in the menu tree. The bullet point color indicates the status of each individual trace profile.
4) Click the name of the desired trace profile in the menu tree. Details about this trace profile are displayed.

25.8.4.24 How to Stop all Trace Profiles

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Profiles** in the menu tree.

4) Click on the **Stop All Trace Profiles** tab.
5) Click on **Stop All** followed by **OK**.

25.8.4.25 How to Add a Trace Profile

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Profiles** in the menu tree.
4) Select one of the following options:
   - If you want to add a blank trace profile, click the **Add Trace Profile (Empty Profile)** tab.
   - If you want to add a trace profile containing the trace components of all trace profiles currently started, click the **Add Trace Profile (with Current Trace Settings)** tab. Select which of the displayed trace components (and with which trace level) should be included in the new trace profile.
5) Enter the name of the new trace profile in the **Profile Name** field.
6) Click on **Apply** followed by **OK**.

25.8.4.26 How to Display Trace Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree.
4) Select one of the following options:
   - If you want to display the list of all trace components, click the **Display All Trace Components** tab.
   - If you want to display the list of all started trace components, click the **Display Started Trace Components** tab.
   - If you want to display the list of all stopped trace components, click the **Display Stopped Trace Components** tab.

25.8.4.27 How to Display Details of a Trace Component

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree. A list of all trace components appears. In addition, the names of all trace components are displayed in the menu tree. The bullet point color indicates the status of each individual trace component.
4) Click on the name of the desired trace component in the menu tree. Details about this trace component are displayed.

25.8.4.28 How to Start or Stop a Trace Component

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree. The names of all trace components are displayed in the menu tree. A red bullet point indicates the trace components that can be started. A green bullet point indicates the trace components that can be stopped.
4) Click on the desired trace component in the menu tree.
5) Click on the **Start/Stop Trace Component** tab.
6) Select one of the following options:
   - To start a trace component, click **Start** and then **OK**.
   - To stop a trace component, click **Stop** and then **OK**.

25.8.4.29 How to Stop all Trace Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree.
4) Click on the **Stop All Trace Components** tab.
5) Click on **Stop All** followed by **OK**.

25.8.4.30 How to Set Trace Settings to Default Values

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree.
4) Click on the **Default Trace Settings** tab.
5) Click the **Default Trace Settings** button followed by **OK** in the next pop up message which notifies you that the action is completed successfully.

NOTICE: Extended tracing increases the general system load and it should not be permanently active. Trace settings should be set back to default by clicking **Default Trace Settings button** as soon as required traces have been successfully created**.**

NOTICE: If extended trace settings are active, you will be notified about this on the home page of the WBM in the **Notifications area. A direct link to the trace settings is also available.**

25.8.4.31 How to Edit Trace Components

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance** > **Traces** in the navigation tree.
3) Click on **Traces** > **Trace Components** in the menu tree.
4) Click on the **Edit Trace Components** tab. A list of all trace components is displayed with the current settings.
5) Change the desired settings.
6) Click on **Apply** followed by **OK**.

25.8.4.32 How to Forward System Log Files automatically

You can enable the option to forward automatically the system log files to an external management system/syslog server.

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click **Maintenance > Traces > Syslog Forwarding** in the navigation tree.

3) Enter the **IP address** and the **Port** of the management system in which the syslog file will be forwarded.
4) Click **Start** to save the configuration changes and initiate the process.

   If the connection with the management portal/syslog server is successful then the **Connection status** has a green circle indicator.

   If the connection with the management/syslog server portal is unsuccessful then the **Connection status** has a red circle indicator.
5) Click **Stop** to deactivate the process.

   The **Connection status** is set to deactivated with a grey circle indicator.
6) If you change the configuration settings, click **Apply** for the changes to take effect.

25.8.4.33 How to Start the Kernel Crash Data Service

Prerequisites

You are logged into the WBM with the **Expert** profile.

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.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click on **Maintenance** > **Traces**.
3) Click on **Trace Components > Kernel Crash Data**.
4) Click on **Start**.

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

Prerequisites

You are logged into the WBM with the **Expert** profile.

Your communication system has an V3 OCC mainboard (OCCLA, OCCMA(R), OCCMB(R).

Step by Step

1) In the navigation bar, click on **Expert mode**.

2) In the navigation tree, click on **Maintenance** > **Traces**.
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 How to Start Media Server Trace

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click on **Maintenance** > **Traces**.
3) Click on **Media Server Trace**.
4) Select an option from the **Trace Level** drop-down list in order to define the level of detail for the trace.
5) Click on **Start**.

NOTICE: Active traces increase the general system load and can have a negative impact on system performance. So, Media Server trace should be disabled as soon as you finish your diagnostic activities.

25.8.4.36 How to Stop Media Server Trace

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert mode**.
2) In the navigation tree, click on **Maintenance** > **Traces**.
3) Click on **Media Server Trace**.
4) Click on **Stop**.

25.9 TCP Dump

A TCP dump is used for monitoring and evaluating data traffic in an IP network.

INFO: Activating a TCP dump can have a negative impact on system performance and must hence only be performed by

experienced administrators and only after consulting with the responsible Service Support.

TCP dump files are stored in the communication system. An appropriate application is required for the diagnosis of the files.

TCP dumps are often used to

- generate a LAN trace for a short period of time (e.g., for a reproducible error image).
- allow authorized service technicians to remotely access a LAN trace.

Advantages over RPCAP daemon: remote access is possible, so trace files do not have to be sent by e-mail

Disadvantages compared to RPCAP daemon: long-term traces are not meaningful; limited storage space, no capture filter can be set, more complex handling for several individual traces

25.9.1 How to Start a TCP Dump

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Traces** > **TCP Dump**.
3) Click on **Start TCP Dump**.
4) Select the desired settings.
5) Click on **Apply** followed by **OK**.

25.9.2 How to Stop a TCP Dump

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Traces** > **TCP Dump**.
3) Click on **Stop TCP Dump**.
4) Click on **OK**.

25.9.3 How to Delete a TCP Dump

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Traces** > **TCP Dump**.
3) Click on **Cleanup TCP Dump**.
4) Click on **Apply**, followed by **OK**.

25.10 RPCAP daemon

An RPCAP (Remote Packet Capture) daemon is used for monitoring and evaluating data traffic in an IP network.

INFO: Activating an RPCAP daemon can have a negative impact on system performance and must hence only be performed by experienced administrators and only after consulting with the responsible Service Support.

The RPCAP daemon enables external applications to remotely access the TCP/IP packets on the LAN interfaces of the communication system.

An RPCAP a daemon is often used for long-term traces, since the trace files are stored on a PC and not in the communication system.

Advantages over TCP dump: faster and easier to use, long-term traces possible, number and/or size of the trace files can be freely selected, trace of internal LAN possible

Disadvantages compared to TCP dump: double network traffic and therefore increased load on the LAN interfaces of the communication system, special opening of ports needed (firewall)

25.10.1 How to Enable the RPCAP Daemon

Prerequisites

You are logged into the WBM with the **Expert** profile.

The RPCAP daemon was disabled.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Traces** > **rpcap Daemon**.
3) Select the desired settings.
4) Click on **Apply** followed by **OK**.

25.10.2 How to Disable the RPCAP Daemon

Prerequisites

You are logged into the WBM with the **Expert** profile.

The rpcap daemon was enabled.

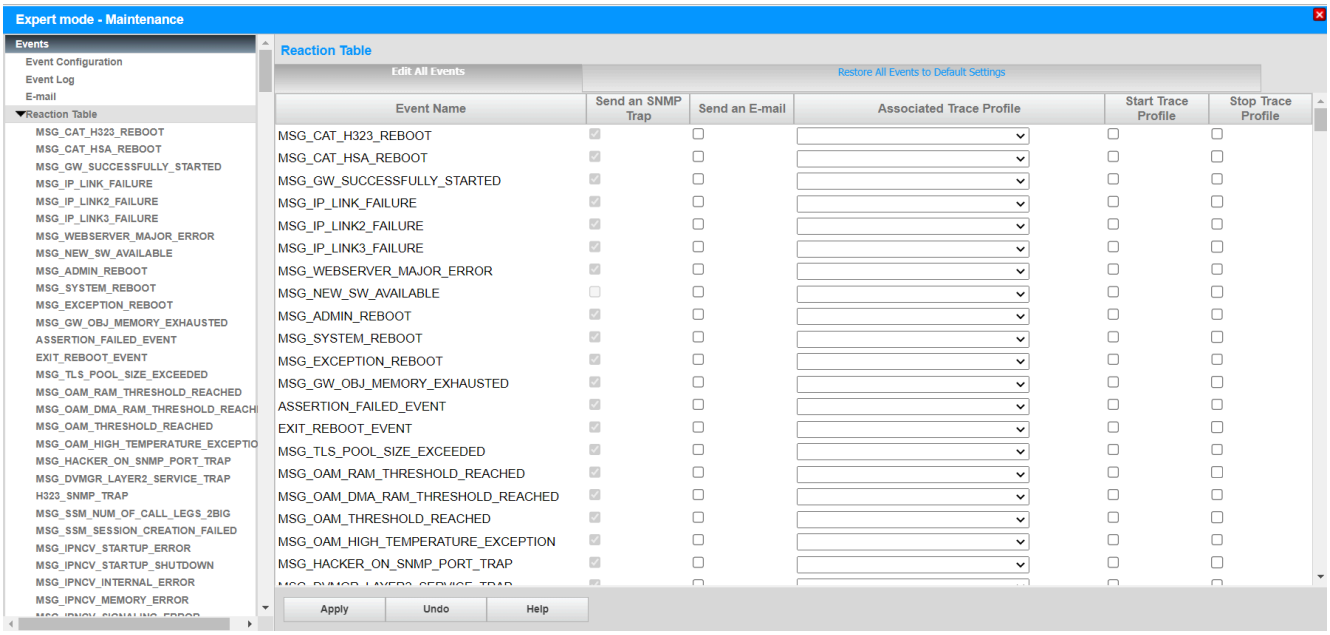
Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Traces** > **rpcap Daemon**.
3) Click on **Apply** followed by **OK**.

25.11 Events

Events provide information about communication system deficiencies. All events are written to a log file that is restricted in size. A new file is created if the maximum file size is exceeded. Up to seven files can be created.

Depending on the setting in the reaction table and the problem class, events may generate an SNMP trap, trigger an e-mail and/or start or stop trace monitoring. The event log (Event Viewer) can be evaluated, configured, and saved via the WBM.



To interpret the event log file, you must download and extract the file with the WBM. The file can then be opened, edited and printed using any text editor. Once the event log file has been transferred, the file can be deleted from the communication system's memory.

Events that can trigger actions are defined by the following properties:

- Event code:

  Identifies an event such as `MSG_ADMIN_LOGGED_OUT` = Logout information of an administrator.

- Event type:

  The following different types exist:

  – Information: plain status messages, no error messages.
  – Warning: report of a possibly problematic procedure or status, but not an error message.
  – Minor: error message. The error has no problematic consequences.
  – Major: error message. This error could cause problems.
  – Critical: Error Message. This error causes problems.
  – Cleared: error message. The error was already corrected by the communication system.
  – Indeterminate: error message. The cause of the error cannot be accurately determined.

- Event text

  Some event texts contain variable data. These are identified in the following manner:

  – %s: character string
  – %u: positive or negative decimal number
  – %f: floating point number
  – %p: indicator (memory address)
  – %x: hexadecimal number (with lower-case letters)
  – %X: hexadecimal number (with upper-case letters)
  – %C: single character
  – %d and %I: positive decimal number

Reaction Table

For each possible event, the Reaction Table can be used by an administrator with the **Expert** profile to independently define what action is to be taken when that event occurs.

You can set whether an SNMP trap should be sent, whether the communication system should be restarted, whether the e-mail should be sent, and whether a trace profile should be started or stopped. If the event is assigned a trace profile, the name of this profile is shown.

E-mail Settings

These settings can be made by an administrator with the **Expert** profile to define how e-mails are sent when an event occurs.

Diagnosis Logs

The communication system logs certain process-specific actions in diagnosis logs. These log files can be evaluated for diagnostic purposes by an administrator with the **Expert** profile.

Alarm Signaling on Exceeding Critical Temperatures

Two critical temperature values are stored in the communication system. If the temperature of the system exceeds the first value, a warning is sent via an SNMP trap or e-mail to indicate that the system temperature is too high. In addition, this message can also be indicated on the displays of up to three system telephones (UP0 & HFA), see How to Define Destinations for Alarm

Signaling. If the second value is exceeded, the boards responsible for the overheating are shut down in a controlled manner (e.g., OpenScape Business Booster Card) or switched off (e.g., SLAV/SLAD). To clear the alarm and put the boards back into service, the system must be switched off and then switched on again.

The 3 destinations (system telephones) to be notified at on exceeding a temperature can be set.

25.11.1 How to Edit Switch Event Logging via a LAN

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Event Configuration**in the menu tree.
4) Select the desired setting.
   - If you want event logging to be transferred via LAN, select the check box **Switch Event Logging via LAN On**.
   - If you do not want event logging to be transferred via LAN, clear the check box **Switch Event Logging via LAN On**.
5) Click on **Apply** followed by **OK**.

25.11.2 How to Download the Event Log File

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Event Log** in the menu tree.
4) Click on the **Load via HTTP** tab.
5) Click on **Load** followed by **OK**. The File Download window appears.
6) Save the file in the desired directory. Then close the window that confirms the download of the file.

25.11.3 How to Delete an Event Log File

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.

2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Event Log** in the menu tree.
4) Click on the **Clear Event Log** tab.
5) Click on **Delete Log** followed by **OK**.

25.11.4 How to Edit E-Mail Settings for Events

Prerequisites

You are logged into the WBM with the **Expert** profile.

E-mail Forwarding must be configured for all systems to use **Emergency Notifications recipient** option. For more information, see How to Configure the Sending of E-mails on page 195

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **E-mail** in the menu tree.
4) Under **Subject**, enter what you want displayed as the Subject field of the e-mail.

   INFO: The subject should state clearly that the e-mail concerns an event.

   ---

5) Enter the e-mail addresses to which the e-mail is sent in the fields **Recipient 1** through **Recipient 5**.
6) Enter the e-mail address of an on-site security officer to which an e-mail is sent when an emergency number is dialed in the **Emergency Recipient** field.

   The subject of the e-mail is "New emergency call". The call number and the name of the caller, if configured, are included in the e-mail which are retrieved from the database of the system.
7) Click on **Apply** followed by **OK**.

25.11.5 How to Display the Event Reaction Table

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Reaction Table** in the menu tree. The reaction table is displayed with all possible events and their settings.

25.11.6 How to Edit the Reaction Settings for an Event

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Reaction Table** in the menu tree. The reaction table is displayed with all possible events and their settings. In addition, the names of all possible events are displayed in the menu tree.
4) Click on the name of the desired event in the menu tree.
5) Click on the **Edit Event** tab. Details on the reaction settings for the desired event are displayed.

INFO: The reaction settings **Reset Gateway** and **Notify OpenScape** cannot be edited. It is not possible to change the **Send an SNMP Trap** setting for all events.

---

6) If possible, select the setting for **Send an SNMP Trap**:
   - If you want an SNMP trap to be sent when the event occurs, enable the check box **Send an SNMP Trap**.
   - Is you do not want an SNMP trap to be sent when the event occurs, disable the **Send an SNMP Trap** check box.
7) Select the setting to **send an e-mail**:
   - If you want an e-mail to be sent when the event occurs, enable the check box **Send an E-mail**.
   - If you do not want an e-mail to be sent when the event occurs, disable the **Send an E-mail** check box.
8) Select the desired trace profile in the **Associated Trace Profile** drop-down list.
9) Select the setting to start or stop the trace profile:
   - If the selected trace profile is to be stopped when the event occurs, enable the check box **Start Trace Profile**.
   - If the selected trace profile is to be stopped when the event occurs, enable the check box **Stop Trace Profile**.
10) Click on **Apply** followed by **OK**.

25.11.7 How to Edit the Reaction Settings for Multiple Events

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.

3) Click on **Events** > **Reaction Table** in the menu tree. The reaction table is displayed with all possible events and their reaction settings.

INFO: The reaction settings **Reset Gateway** and **Notify OpenScape** cannot be edited. It is not possible to change the **Send an SNMP Trap** setting for all events.

---

4) Change the reaction settings for the events you want in the reaction table:
   - If possible, select the setting for **Send an SNMP Trap**:

     If you want an SNMP trap to be sent when the event occurs, enable the check box **Send an SNMP Trap**.

     Is you do not want an SNMP trap to be sent when the event occurs, disable the **Send an SNMP Trap** check box.
   - Select the setting to **send an e-mail**:

     If you want an e-mail to be sent when the event occurs, enable the check box **Send an E-mail**.

     If you do not want an e-mail to be sent when the event occurs, disable the **Send an E-mail** check box.
   - Select the desired trace profile in the **Associated Trace Profile** drop-down list.
   - Select the setting to start or stop the trace profile:

     If the selected trace profile is to be stopped when the event occurs, enable the check box **Start Trace Profile**.

     If the selected trace profile is to be stopped when the event occurs, enable the check box **Stop Trace Profile**.
5) Click on **Apply** followed by **OK**.

25.11.8 How to Download or Open Diagnosis Logs

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Diagnosis Logs** in the menu tree.
4) Click on the **Get Diagnosis Logs** tab. You will see a list of all available logs with the respective file name, file size in bytes, time of last activation and file attributes.
5) Click under **File Name** of the name of diagnosis log you want. The File Download window appears.
6) Save the file in the desired directory. Then close the window that confirms the download of the file.

25.11.9 How to Clear Diagnosis Logs

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Diagnosis Logs** in the menu tree. You will see a list of all available logs with the respective file name, file size in bytes, time of last activation and file attributes.
4) Click on the **Delete Diagnosis Logs** tab.
5) Click on **Delete Log** followed by **OK**.

25.11.10 How to Define Destinations for Alarm Signaling

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) Click on **Maintenance** > **Events** in the navigation tree.
3) Click on **Events** > **Alarm Signaling** in the menu tree.
4) In the **Stations 1-3** drop-down lists, select the three destinations (system telephones with display, UP0 & HFA) where a notification is to be displayed when the system temperature exceeds a preset critical value.
5) Click on **Apply**, followed by **OK**.

25.12 Configuration Data for Diagnostics

"Smaller" backup sets containing diagnostic data for Service Support can be created for diagnostic purposes. In contrast to normal backup sets, significantly smaller data amounts are produced for this purpose and can thus be easily sent with an e-mail, for example.

Diagnostics backup sets include, among other things, the configuration data of the communication system and the UC Application (UC Smart or UC Suite). Voicemails, fax messages and announcements are not included.

The following media can be used to save backup sets for diagnostics:

- **USB Device**

  The data can be backed up to a connected USB drive or a connected USB stick, for example.

  NOTICE: If a USB hard disk, a partition thereof, or a USB stick is to be used for the backup, it must be formatted with FAT 32. Due to filesystem limitation, the maximum size of

the backup set cannot exceed 4 GB. In such cases, alternate backup media must be selected. USB media formatted with NTFS are read-only. Note that if multiple partitions exist, only the first partition can be used for the backup.

If a bootable USB device is used for the backup, this USB device must be safely removed after the backup.

- **HTTPS**

  The data can be saved via HTTPS on the hard disk of the client PC.
- **Hard Disk** (only for OpenScape UC X3/X5/X8 UC Booster Card (OCAB Application Board))

  The data can be saved on the hard disk of the OCAB Application Board.

INFO: It is not possible to create a backup on the hard disk of the communication system.

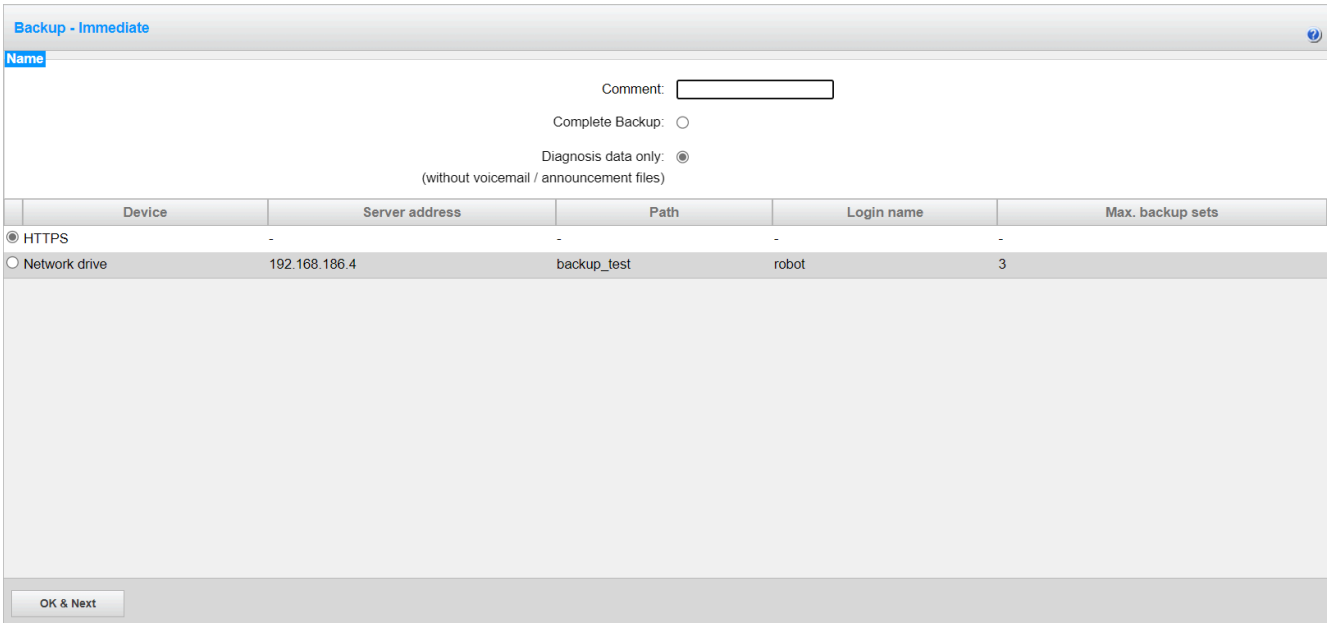
25.12.1 How to Generate Configuration Data for Diagnostics

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Data Backup** in the navigation bar.
2) In the navigation tree, click **Data Backup** > **Backup - Immediate**.



3) Enable the **Diagnostics** check box.

4) Select the device on which the diagnostics backup set is to be saved You have the following options:
   - If you want to save the data on a connected USB drive or a connected USB stick, enable the **USB Device** radio button.
   - If you want to back up the data using HTTPS on the hard disk of the client PC, enable the **HTTPS** radio button.
   - Only for OpenScape Business X3/X5/X8 with UC Booster Card (Application Board OCAB): If you want to save the data on the hard disk of the Application Board OCAB, select the **Hard Disk** radio button.
5) If required, enter a comment for your diagnostics backup set in the **Comment** field. Avoid the use of diacritical characters such as umlauts and special characters in your input.
6) Click on **OK & Next**. The progress of the backup process is displayed in a separate window.
7) The backup was successful if the message `Backup complete!` appears.
8) If you have selected **HTTPS** as a backup medium, you must save the diagnostics backup set and the associated text file with to a location of your choice. This is done automatically for the other backup media. The browser window must remain open until the save operation for the diagnostics backup set and text file has been completed.

   NOTICE: If you selected **USB Device** as a backup medium, wait till the LED of the USB device stops flashing. It is only then that the diagnostics backup set has been completely stored on the USB device. You can then remove the USB device.

9) Click on **Finish**.

Next steps

The diagnostics backup set can now be sent to the responsible Service Support by e-mail to assist in the troubleshooting process, for example.

25.13 Card Manager

OpenScape Business is supplied with bootable mediums that contain the system software. The Card Manager is a tool intended for service support to create a new system software on an empty SDHC card, M.2 SATA SSD and UC Booster Card Hard disks (HDD). To do this, the software of the communication system must be available as a compatible image file.

The software on the SDHC card, M.2 SATA SSD or HDD is standard system software without customer data. It cannot be used for software updates or for backing up customer data. It is possible only in the case of the SDHC card to include a backup file during creation.

The Card Manager can be launched as an ISO image in a Linux boot DVD, a Linux Bootable USB stick or in a Virtual Environment.

The Card Manager software is available via the Partners Portal

Use Cases

- Before delivery of the system, the software should be replaced with the latest software version.
- The storage device is defective and must be replaced by a new on which no software has yet been stored.
- The used software is corrupted and needs to be reloaded. All customer data is deleted in the process.

  If a backup set exists for the recovery of the customer data, the newly installed software should match the software version with which the backup set was created so that the settings contained in the backup set can also be supported and processed by the installed software.

25.13.1 How to Use the Card Manager to Write the Communication Software on the M.2 SATA SSD

You can use the Card Manager to write the communication software of OpenScape Business V3 on M.2 SATA SSD.

Prerequisites

The working memory of the PC should be at least 3 GB.

PC with a Windows 10 operating system DVD drive and at least 2 USB 2.0 or higher interfaces are available.

Card Manager Tool V3 or higher which is fully operational on a PC.

USB SATA SSD adapter is available. The adapter must have Key M and Key B support.

A qualified M.2 SATA SSD is available.

A System SW image in the correct version is available as a tar file. The SW version should match the version of the target system. It must be exactly the same version that is in use in the current storage device of the system.

Card Manager application as a DVD ISO file.

The Card Manager ISO file has to be burned to a DVD.

Step by Step

1) Store the current image tar file on a USB stick and boot the Card Manager application from the DVD ISO file.

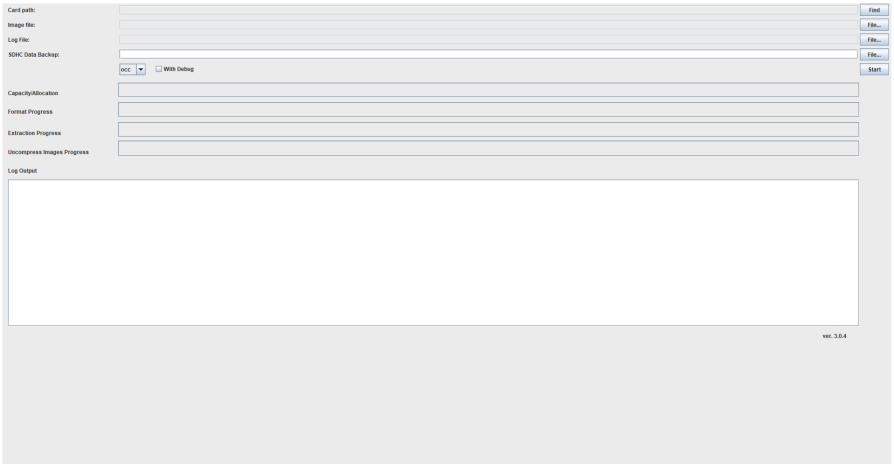
2) Connect the USB SATA SSD adapter into a USB port on the PC .

3) Insert the M.2 SATA SSD in the adapter and click **OK** on the pop-up to confirm the selection.

All data on the inserted SSD will be deleted by the Card Manager.

Do not insert any additional USB device to the PC, as it will be recognized as an OpenScape Business storage medium and all data will be deleted.

4) On the Card manager application, click **Find** next to **Card path**.



5) Insert USB stick with the image file and click on **File...** next to the **Image file** and select the image tar file stored on the USB Stick.

6) Select **OCCe** from the drop-down menu for creating the M.2 SATA SSD.

7) Optionally, you can also create a log file that records any program errors that may have occurred. To do this, click on **File...** next to **Log File** and navigate to the storage location of the log file. Enter a name for the log file and click on **Save**.

8) Click on **Start**.

   The write process is started and the progress of each step is displayed via a progress bar.

9) Click on **OK** once the installation is completed and remove the M.2 SATA SSD from the adapter.

10) Remove the adapter from the USB port.

11) Power off the communication system.

12) Insert the new M.2 SATA SSD into the switched off communication system.

13) Turn on the communication system. The system starts with the new M.2 SATA SSD, the same software version and configuration and is ready for operation when the green LED flashes at 1Hz (0.5 sec on / 0.5 sec off).

NOTICE: If the M.2 SATA SSD is inserted in an OpenScape Business communication system, the system is started in the factory default state including, among other things, the default IP address `192.168.1.2`.

Restore a backup of the system. The backup should have the same minor version with the installed system.

25.13.2 How to Use the Card Manager to Write the Communication Software on the SDHC Card

You can use the Card Manager to write the communication software of OpenScape Business V3 on an SDHC Card.

Prerequisites

PC with a Windows 10 operating system DVD drive and at least 2 USB 2.0 or higher are available.

Card Manager Tool V3 or higher which is fully operational on a PC.

USB SDHC card reader is available.

A qualified SDHC card is available.

Optional a SDHC Data Backup file (tar file) stored on a USB stick together with the image system.

The write protection of the SDHC card is disabled.

A System SW image in the correct version is available as a tar file. This can be either the small (OCC) or the big (OCAB) image file. The SW version should match the version of the target system. It must be exactly the same version that is in use in the current SDHC card of the system.

Card Manager application as a DVD ISO file.

The Card Manager ISO file has to be burned to a DVD.

Step by Step

1) Store the current image tar file on a USB stick and boot the Card Manager application from the DVD ISO file.

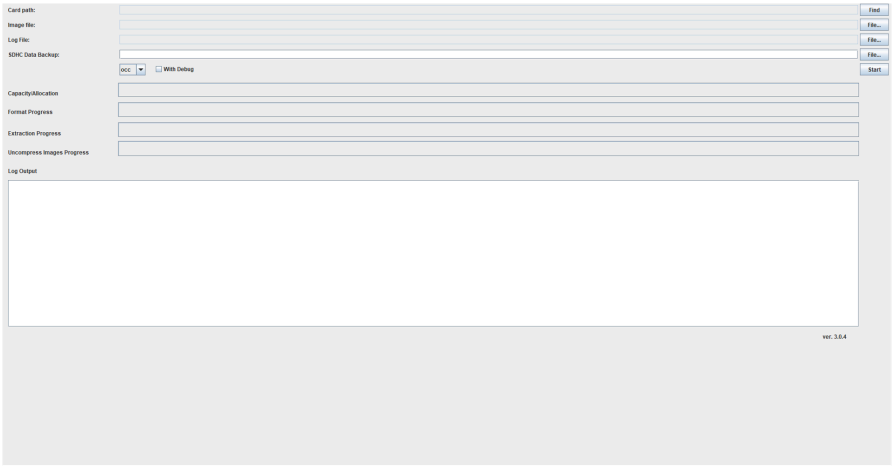
2) Connect the USB SDHC card reader into a USB port of the PC.

3) Unplug the card reader, insert the SDHC card, plug in the card reader again and click **OK** on the pop-up window. The path of the SDHC card appears under **Card path**.

All data on the inserted SSD will be deleted by the Card Manager.

Do not insert any additional USB device to the PC, as it will be recognized as an OpenScape Business storage medium and all data will be deleted.

4) On the Card manager application, click **Find** next to **Card path**.



5) Insert USB stick with the image file and click on **File...** next to the **Image file** and select the image tar file stored on the USB Stick.

6) Select **OCC** from the drop-down menu for creating the SDHC card.

7) Optionally, you can also create a log file that records any program errors that may have occurred. To do this, click under **Log File** on **File...** and

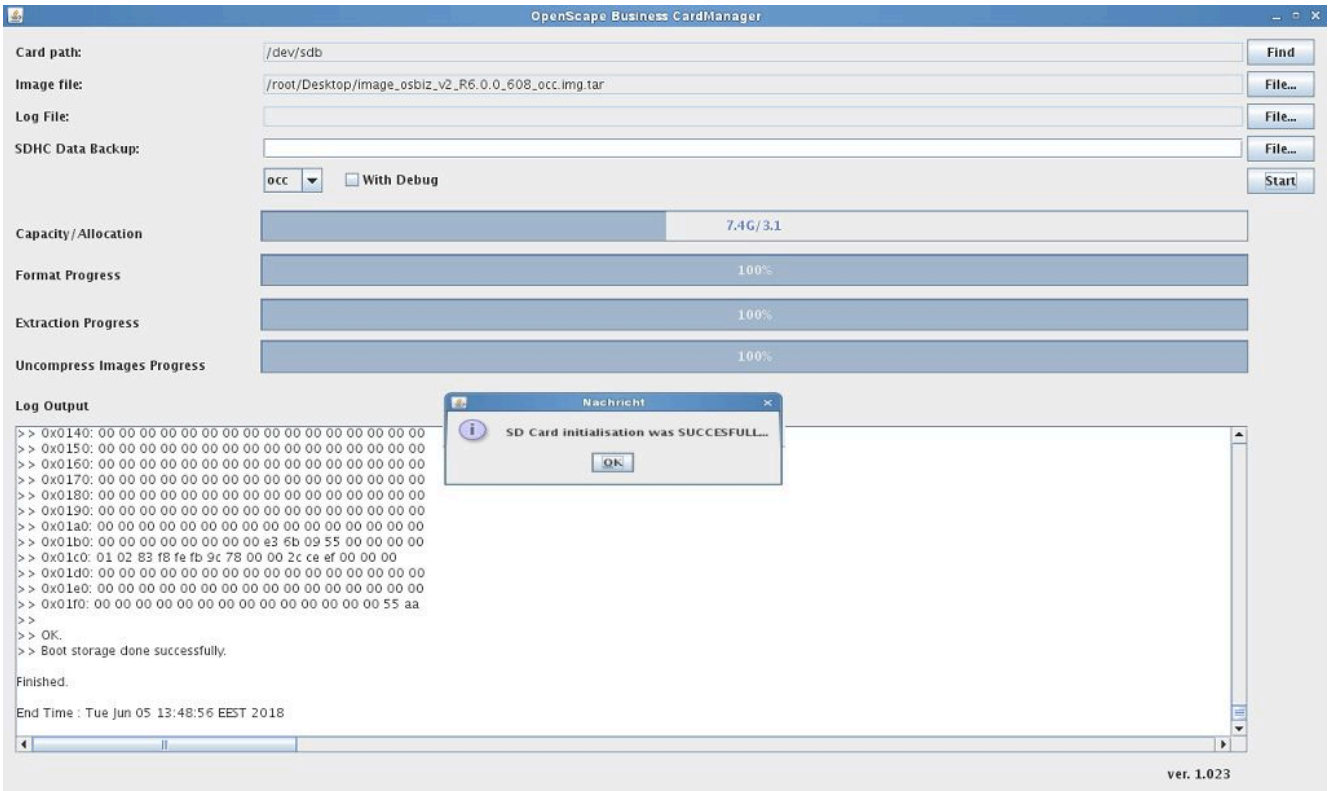
navigate to the storage location of the log file. Enter a name for the log file and confirm it with **Save**.

8) Optionally, click under **SDHC Data Backup** on **File...** and select the .tar file with a customer specific SDHC Card Data Backup file. The path to the .tar file appears under **SDHC Data Backup.**

9) Click on **Start**.

The write process is started and the progress of each step is displayed via a progress bar.

NOTICE: If the text field (**SDHC Data Backup**) is filled, Card Manager will firstly compare the version of the SDHC Card Backup file with the version of the system SW image file. In case of a mismatch an error message is displayed and the process is aborted. In case of a match, the Card Manager writes the selected image and then extracts the specified .tar file in the SDHC. If no SDHC Data Backup is available, the text field should remain empty.



10) Click on **OK** once the installation is completed and remove the SDHC card from the card reader.

11) Remove the card reader from the USB port.

12) Power off the communication system.

13) Insert the new SDHC card into the SD slot of the switched off communication system.

14) Turn on the communication system. The system starts with the new SDHC card and with the same software version and configuration and is ready for operation when the green LED flashes at 1Hz (0.5 sec on / 0.5 sec off).

NOTICE: If the SDHC card is inserted in an OpenScape Business communication system, the system is started in the factory default state including, among other things, the default IP address `192.168.1.2`.

25.13.3 How to Use the Card Manager to Write the Communication Software on the OCAB hard disk

You can use the Card Manager to write the communication software of OpenScape Business V3 with OCAB on OCAB hard disk.

Prerequisites

PC with a Windows 10 operating system DVD drive and at least 2 USB 2.0 or higher interfaces are available.

Card Manager Tool V3 or higher which is fully operational on a PC.

An adapter for the OCAB hard disk is available. The adapter must have Key M and Key B support.

A qualified OCAB hard disk is available.

A System SW image (OCAB) in the correct version is available as a tar file. The SW version should match the version of the target system. It must be exactly the same version that is in use in the current storage device of the system.

Card Manager application as an ISO file.

The Card Manager ISO file has to be burned to a DVD.

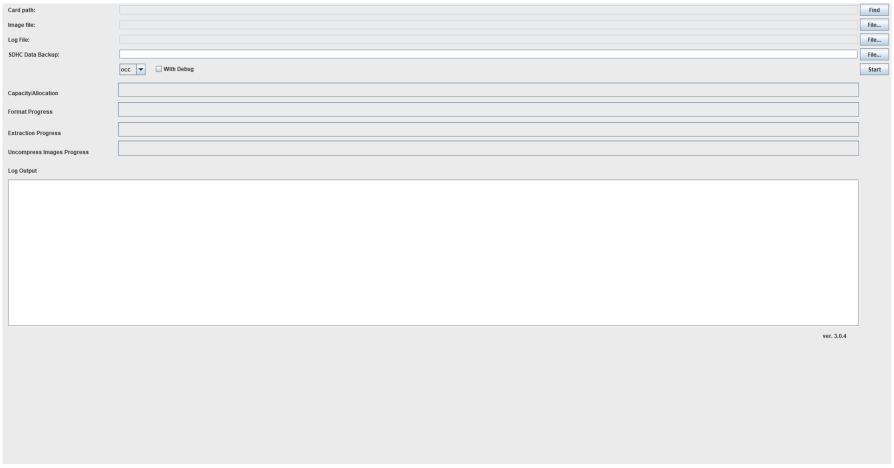
Step by Step

1) Store the current image tar file on a USB stick and boot the Card Manager application from the DVD ISO file.
2) Connect the adapter into a USB port on the PC .
3) Insert the OCAB hard disk in the adapter and click **OK** on the pop-up to confirm the selection.

   All data on the inserted hard disk will be deleted by the Card Manager.

   Do not insert any additional USB device to the PC, as it will be recognized as an OpenScape Business storage medium and all data will be deleted.

4) On the Card manager application, click **Find** next to **Card path**.



5) Insert USB stick with the image file and click on **File...** next to the **Image file** and select the image tar file stored on the USB Stick.
6) Select **OCAB** from the drop-down menu for creating the OCAB hard disk.
7) Optionally, you can also create a log file that records any program errors that may have occurred. To do this, click on **File...** next to **Log File** and navigate to the storage location of the log file. Enter a name for the log file and click on **Save**.
8) Click on **Start**.

   The write process is started and the progress of each step is displayed via a progress bar.
9) Click on **OK** once the installation is completed and remove the OCAB hard disk from the adapter.
10) Remove the adapter from the USB port.
11) Power off the communication system.
12) Mount the new OCAB hard disk into the UC Booster Card and then insert it in the switched off communication system.
13) Turn on the communication system. The system starts with the new OCAB hard disk, the same software version and configuration and is ready for operation when the green LED flashes at 1Hz (0.5 sec on / 0.5 sec off).

NOTICE:

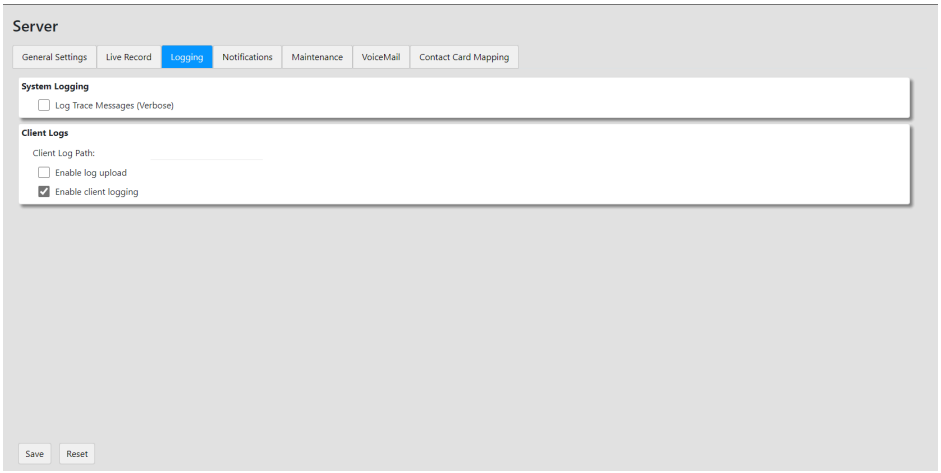
All customer media data are lost. You can do a restore of a system backup set to get these data back.

25.14 Monitoring and Maintaining the UC Suite

The WBM **Expert** profile offers administrators numerous functions for monitoring and maintaining the UC Suite.

25.14.1 Logging

The execution of the UC Suite is monitored internally by the system. **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**.



System Logging

The following system logs can be enabled or disabled:

System log	Default setting
Log Trace Messages (Verbose)	Not activated

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`.

INFO: The analysis of these log files can only be performed by Development.

Client Logs

Client Logs are the log files of the UC Suite. For each UC Suite client (myPortal for Desktop, myAttendant, etc.) and station (user), a separate directory is created, and the relevant log files are stored in it. The logs record the activities of a subscriber such as starting the client, outgoing and incoming calls, etc.

INFO: The storage of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.

The path in which the `CC-Logs` directory with the subdirectories for the individual UC Suite clients is to be stored can be defined. You can also select whether the directory is to be stored on every client PC or on a central PC or server on the network.

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. No changes are possible.

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**.

Depending on the scenario, the client logs are also stored by default on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system. 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 How to Enable or Disable Recording of System Logs

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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) Click on **Save**.

25.14.1.2 How to Enable or Disable the Recording of Client Logs on a System-wide Basis

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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.

   INFO: The recording of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.

5) Click on **Save**.

25.14.1.3 How to Enable or Disable the Recording of Client Logs on a Station-specific Basis

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) In the navigation bar, click on **Setup**.
2) Click in the navigation tree on **Wizards** > **UC Suite**.
3) Click on **Edit** to start the **User Directory** wizard.
4) Mark the desired station in the user directory and click **Edit**.
5) Click on **My Preferences** > **Miscellaneous** in the menu tree.
6) Select one of the following options:
   - If client logs are to be recorded for the desired subscriber, select the **Log Debug Messages (Verbose)** check box.
   - If you do not want client logs are to be recorded for the desired subscriber, clear the **Log Debug Messages (Verbose)** check box.

   INFO: The recording of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.

7) Click on **Save**.
8) If you want to enable or disable the recording of client logs for further subscribers, repeat steps 4 through 7.

25.14.1.4 How to Configure the Storage Path for Client Log Files

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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. Select one of the following options:
   - 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>`.

   INFO: The storage of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.
5) Click on **Save**.

25.14.1.5 How to Enable or Disable Central Storage of Client Logs on the Hard Disk of the Communication System

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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.

   INFO: The recording of client logs is supported only for the UC Suite clients used with Microsoft Windows operating systems.
5) Click on **Save**.

25.14.1.6 How to Download the Client Logs of all Internal Stations

The **Trace** wizard can be used to download client logs (log files) of the UC Suite clients (myPortal for Desktop, myAttendant, etc.) used by internal subscribers. Client logs are supported only for the UC Suite clients used with Microsoft Windows operating systems.

Prerequisites

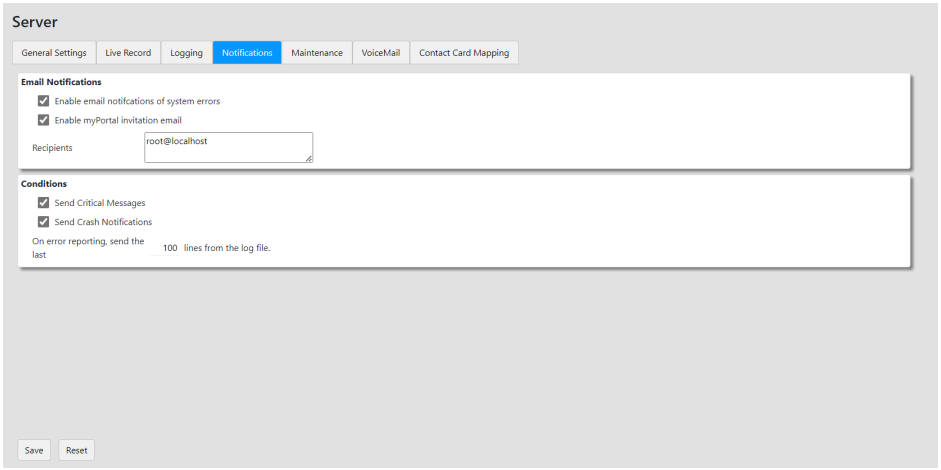
You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click **Diagnostics** > **Trace** in the navigation tree.
3) Click on **Diagnosis Logs**.
4) Click on **No Log** to clear the check boxes of all logs.
5) Select the check box **Application Protocols**.
6) Select one of the following options:
   - If you want to download the entire existing log, select **Complete Trace Log** in the drop-down list.
   - If you want to download the log for today, select **Log from Today** in the drop-down list.
   - If you want to download the log for a specific time period, select **Own Selection** in the drop-down list. Then, select the beginning and end of the desired time period in the drop-down lists **From:** and **To:**.
7) Click on **Load** followed by **OK**. The File Download window appears.
8) Save the file in the desired directory. Then close the window that confirms the download of the file.
9) Click on **Next** followed by **Finish**.

25.14.2 Notification

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**:

Conditions	Default setting
Send Critical Messages	Enabled
Send Crash Notifications	Activated

The Send Critical Messages and Send Crash Notifications settings should be enabled and thus sent. These messages warn the entered recipients about a potential problem that needs to be reported to the responsible Service Support.

In addition, you can define how many of the last lines of a log file should be included with the sent e-mail. The following system errors can be reported (in English only):

System error
NULL monitor
Could not notify Call Handler
Terminate call failed
Unable to load VM Structure from file
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle
Database connection failed
Rules engine logic failure
Config schema format failure
90% Disk usage mark
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.
Database logic error
Database schema error
Connection Server failed to start
MultisiteSync failed to start
Multisite failed to start
TransferManager failed to start
IPC failed to start
ConferenceManager failed to start
CallManager failed to start
MediaProcessing failed to start
Queues failed to start
Import failed to start
Data client failed to start
DirectoryClient failed to start

System error
DirectoryServer failed to start
FV failed to start
IM failed to start
Switch failed to start
No Switches
Exchange Integration failed to start
Outbound Fax failed to start
SQL connection pool failed to start
Task scheduler failed to start
Trunks failed to start
Unknown switch type
Users failed to start
MEB has been disconnected
MEB ACK timeout
Switch Heartbeat timeout

25.14.2.1 How to Configure E-mail Notifications of System Errors

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Notifications**.
4) Select the desired setting for the e-mail notification, under the **Email Notifications** area:
   - If you want e-mail notifications, activate the **Enable e-mail notifications of system errors** check box.
   - If you do not want e-mail notifications, clear the **Enable e-mail notifications of system errors** check box.
5) Enter the e-mail addresses of the individuals to whom e-mail notifications are to be sent in the **Recipients** field. Different email addresses must be separated by a comma "," followed by space " ".
6) Select the desired setting for critical messages
   - If you do want e-mail notifications for critical messages, activate the **Send Critical Messages** check box.
   - If you do not want e-mail notifications for critical messages, clear the **Send Critical Messages** check box.

7) Select the desired setting for crash notifications
   - If you do want e-mail notifications for system crashes, activate the **Send Crash Notifications** check box.
   - If you do not want e-mail notifications for system crashes, clear the **Send Crash Notifications**.
8) Enter the number of log file lines to be sent with an e-mail in the **Send Lines of Log File** field.
9) Click on **Save**.

25.14.3 Maintenance

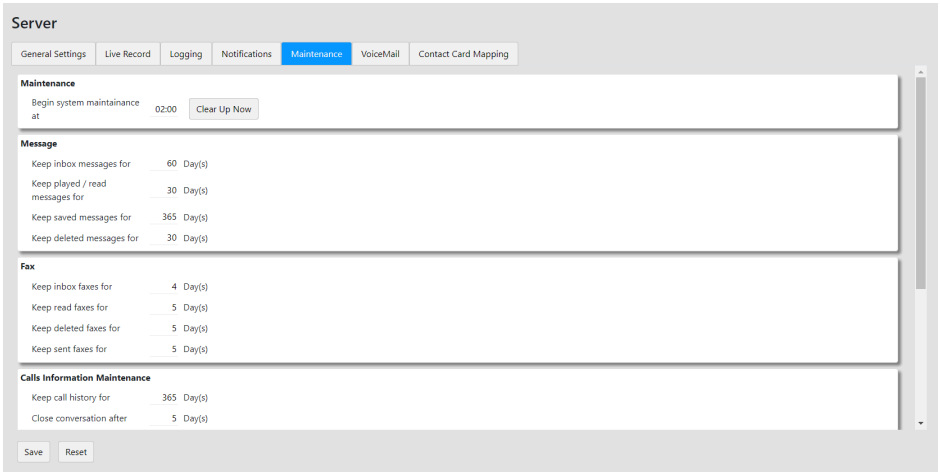
Retention periods can be defined via the Maintenance for messages, for call information in the Call Journal, for calls recorded with myAgent, for faxes and e-mails received and sent for the Contact Center and for log files.

You can also set at what time the following data for which the set retention periods have expired is deleted on a daily basis:

- Messages
- Call information in the call journal (call history)
- Calls recorded with myAgent (contact center)
- Faxes and e-mails received and sent for the Contact Center
- Log files

The default setting is 2:00 a.m.

In addition, it is also possible to start the system maintenance immediately and to thus initiate the immediate deletion of the above data for which the respectively set retention periods have expired. This may be necessary, for example, if the hard disk capacity of the communication system has reached a critical level.



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. The default setting for the retention period for contact center data is 60 days.

INFO: The retention periods for the maintenance of the call information are independent of one another.

Contact Center reports are based on the call history. If a shorter retention period was set for the call history than for the contact center data, some reports may no longer be available.

During **Log File Maintenance**, the log files for which the set retention periods have expired are deleted. The default setting for the retention period for log files is 10 days.

25.14.3.1 How to Configure the Time for Maintenance

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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. Routine system maintenance tasks such as deleting messages, call information in the call journal, and log files for which the set retention periods have expired will then be initiated at the time specified here.
5) Click on **Save**.

25.14.3.2 How to Configure Retention Periods for Log Files

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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. Log files are deleted when the retention period specified here expires.
5) Click on **Save**.

25.14.3.3 How to Perform Immediate System Maintenance

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **OpenScape Business UC Suite**.
3) Click on **Server** followed by **Maintenance**.
4) Click on **Clear Up Now**, under the **Maintenance** area.

   INFO: The following items for which the set retention periods have been exceeded are deleted: messages, call information in the call journal, calls recorded with myAgent, received and sent faxes and e-mails for the contact center and the log files.

5) Click on **OK** to confirm the deletion.

25.14.3.4 How to Configure the Retention Period for Contact Center Data

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **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. The calls recorded with myAgent and the received and sent faxes and e-mails for the contact center will be deleted if they have exceeded the retention period set here.
5) Click on **Save**.

25.15 Monitoring the UC Smart

Administrators can query the current status of the UC Smart using the WBM in **Expert** mode.

25.15.1 How to Query the Current Status of UC Smart

Prerequisites

You are logged into the WBM with the **Expert** profile.

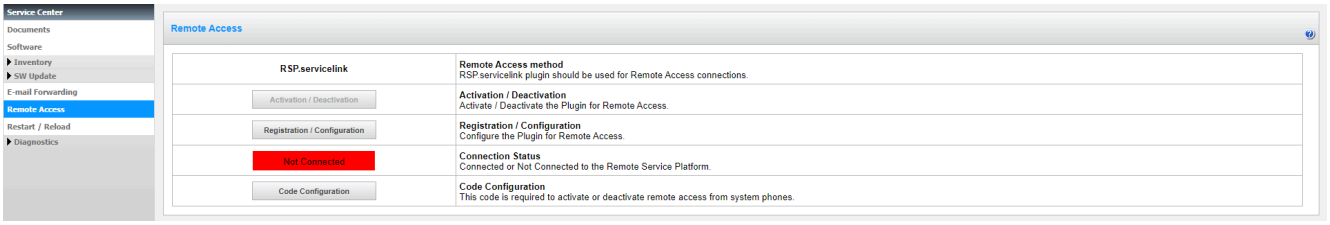
Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Applications** > **UC Smart**.
3) Click on **Status**.

   The current status of the application server and the number of active connections for each UC client is displayed.

25.16 Remote Services

Different Remote Services provide remote access to the communication system and the connected components to authorized service technicians. This reduces the cost of maintenance activities, while still providing users with on-site support in solving their problems.



Due to the highest level of security, the RSP.servicelink should be given precedence over Remote Service. For more information see RSP.servicelink.

25.16.1 RSP.servicelink

Remote access with RSP.servicelink connectivity (**R**emote **S**ervice **P**latform) offers authorized service technicians of a Remote Service Partner the option to remotely administer the communication system as well as the UC Booster applications comfortably and securely from a distance. To configure RSP.servicelink, only an Internet connection, a web browser, the partner ID and the parner password of the remote service partner are required. RSP.servicelink ensures a broadband connection with high security.

RSP.servicelink is based on OpenVPN technology. It uses the SSL/TSL protocol and encryption and provides the highest level of security with an additional client certificate.The term RSP.servicelink is abbreviated to RSP in the documentation.

NOTICE: RSP is using the range 100.64.0.1 - 100.127.255.254 for the tun0 interface, when RSP is active, which means that if an external IP within this range needs to be accessed, a static route should be added in the Open Scape Business system to route the traffic through the desired interface.

RSP offers the following major advantages in combination with OpenScapeBusiness:

- High security through outbound Internet connection

  The entire remote connection setup is always initiated by the communication system. This means that the firewall of the customer network must only allow one HTTP connection to a single address in the Remote Service Center (port 443). Under normal circumstances, no change is required in the security policies of customers or their firewalls, since this port is usually already open for outbound internet call in the firewall of the customer. High security for the customer network is thus guaranteed.

  With RSP, the administrator of the communication system retains control over the remote connection by simply enabling and disabling access. In the case of RSP.servicelink, a client certificate is automatically installed as well.
- High bandwidth

  Due to the broadband Internet connection, diagnostics data can be transmitted much faster, thus increasing the quality of service.
- Simple and cost-effective setup

  The software of the communication system already includes a so-called RSP.servicelink. When activating the service plugin, the partner ID of the Remote Service Partner and also the partner password must be entered.

  Every remote service partner who uses the RSP.servicelink has a separate partner ID.

  The RSP.servicelink plugin should be deactivated and then reactivated when a software update is going to be performed.
- Future-proof

  RSP is the basis for future (value-added) services such as automated backups, reporting and monitoring, for example.

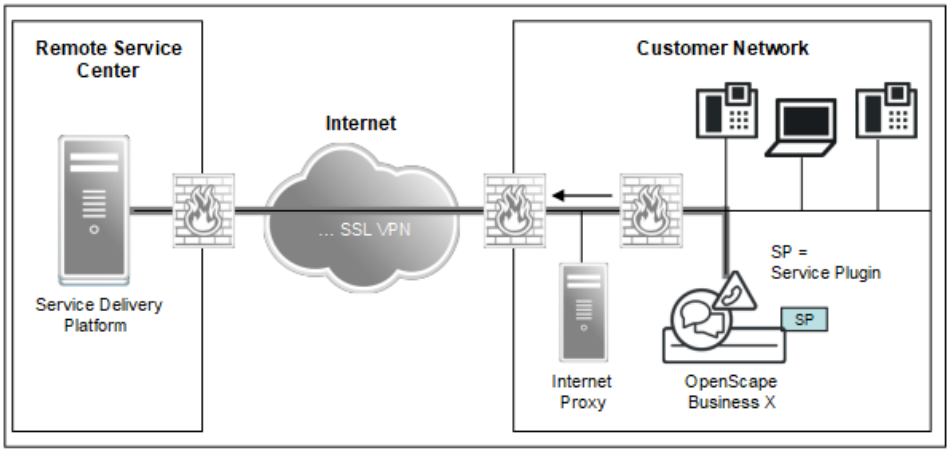


Figure 17: RSP - Overview for OpenScape Business X

RSP supports all the usual Web Services Standards, including the Hypertext Transfer Protocol Secure (HTTPS), Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML).

Communication between the client side and the Remote Service Center is always secured with an AES-256-CBC encryption for RSP.servicelink.

Service Plugins

The RSP.servicelink plugin can be enabled or disabled individually.

The RSP.servicelink plugin must be reset after the mainboard has been replaced, for example. Resetting the service plugin deletes the entire RSP configuration and disables the plugin.

NOTICE: In case the system is not in DTAG mode and the RSP.servicelink plugin is active, it is not possible to change the proxy settings configuration. The **Registration / Configuration button is disabled.**

In DTAG mode, if RSP.servicelink plugin is active, pressing Registration / Configuration button shows directly Proxy Settings page with Abort/Finish buttons. This is also possible from the remote server.

Device Management (Managed Device)

In communication systems without a UC Booster, remote access to further devices in the customer LAN can be enabled by configuration on the SIRA side. IP phones can be configured on the SIRA side by using the "Managed Devices" function.

INFO: Remote access to other OpenScape Business communication systems in the customer LAN is not possible. Each OpenScape Business must be configured for remote access.

Activating/Deactivating

The following options are available for activating or deactivating the service plugins:

- Using the **Activation / Deactivation** wizard

  There is a separate activation/deactivation wizard for the RSP service plugins.
- By entering a code at the system telephone (default: activation via *996, deactivation via #996)

  For security reasons, a 4-digit PIN must be entered in addition to the code for the activation and deactivation via a system telephone. The configuration of this PIN is performed in the WBM of the communication system with the **Advanced** profile.

Backup and Restore

RSP credentials are stored in the backup set of the system.

If a new OpenScape Business system is set up via cloning or via data restore (migration), and the original system had RSP access configured, it has to be ensured that the cloned or restored system has a different RSP configuration active.

You have to deactivate or uninstall the RSP before cloning or backing up the original system.

If a certificate for connecting to RSP is used in more than one systems, then the certificate will be revoked and none of the OpenScape systems will be ale to connect to RSP service.

Prerequisites

- Internet access for the communication system or the HTTP proxy in the customer LAN.
- Any existing firewall in the customer LAN must be opened for Registrar:
  - https://188.64.18.51
  - https://188.64.17.51
- Any existing firewall in the customer LAN must be opened for VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- A default router must be specified in the Internet configuration.

NOTICE: In case the system is in DTAG mode during system startup and has internet access without the RSP.serviceplugin being installed and configured, then a script will automatically install, configure and activate RSP.serviceplugin using the PartnerID and password for DTAG (device name will be the MAC address of the system). The script will also be called periodically every 10 minutes (e.g for the case where is no internet access after initial system installation). The script will not activate automatically RSP.serviceplugin in case the user has manually deactivated it.

25.16.1.1 How to Install, Configure and Register the RSP.servicelink Plugin

The **Registration / Configuration** wizard can be used to install, configure and register the RSP.servicelink Plugin for remote access to the communication system using RSP.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.

2) Click on **Remote Access** in the navigation tree.

3) Click on **Registration / Configuration**.

4) If the RSP.servicelink plugin is not yet installed, click on **Install** and then on **OK & Next**.

5) If the RSP.servicelink plugin is already installed, click **OK & Next**.

6) If no proxy server is used in the customer network, click **OK & Next**, since the **Proxy Parameters** do not need to be configured. Skip the next two steps.

7) If a proxy server is used in the customer network, you must select the **Proxy Parameters** setting depending on the customer network:

- If a proxy with the HTTP protocol exists in the customer network, select the **Enable HTTP Proxy** check box. Enter the host name on the **HTTP Proxy Host** field and the port number of the proxy server in the **HTTP Proxy Port** field. If required, enter the user name and password

required for the authentication at the proxy server in the **User Name** and **Password** fields.

- If a proxy with the SOCKS protocol exists on the customer network, select the **Enable SOCKS Proxy** check box. Enter the host name on the **SOCKS Proxy Host** field and the port number of the proxy server in the **SOCKS Proxy Port** field. If required, enter the user name and password required for the authentication at the proxy server in the **User Name** and **Password** fields.

  INFO: The type and configuration of the proxy server determines whether or not authentication is required.

8) Click **OK & Next**.
9) Change the preset partner ID in the **Partner ID** field only if required.
10) Enter your password in the **Password** field.
11) Enter the device name. You can find the device with the device name in the SIRA Equipment Explorer (EqE). The MAC address of the OpenScape Business is the default entry.
12) Click **Finish.**

The **Connection Status** row in the **RSP.servicelink** column indicates whether the registration was successful. In the event of an unsuccessful registration, the following error messages may be displayed:

- MAC already registered:

  Solution: Delete the device (= OpenScape Business communication system) on the SIRA Equipment Explorer and register it again with the **Registration / Configuration** wizard.

  NOTICE: You can find the device on the SIRA Equipment Explorer through the device name or the MAC address. The device name or the MAC address of the OpenScape Business communication system can be found in the **Service Center** under **Remote Access**.

- Configuration Error:

  Solution: Re-enter the Partner ID and Password in the **Registration / Configuration** wizard and exit the wizard correctly.
- Wrong Credentials:

  Solution: Re-enter the Partner ID and Password in the **Registration / Configuration** wizard and exit the wizard correctly.

25.16.1.2 How to Enable the RSP.servicelink Plugin

The **Activation / Deactivation** wizard can be used to disable the RSP.servicelink Plugin for remote access to the communication system using RSP.

Prerequisites

A functioning DNS configuration is available.

A default router for Internet access or, alternatively, a proxy server in the customer network is available.

The RSP.servicelink Plugin is deactivated.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click in the **RSP.servicelink** column on **Enable / Disable**.
4) Click **Activate**.

25.16.1.3 How to Disable the RSP.servicelink Plugin

The **Activation / Deactivation** wizard can be used to disable the RSP.servicelink Plugin for remote access to the communication system.

Prerequisites

The RSP.servicelink plugin is enabled.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click on **Enable/ Disable in** the **RSP.servicelink** column.
4) Click on **Deactivate**.

25.16.1.4 How to Reset the RSP Service Plugin

The **Activation / Deactivation** wizard can be used to reset the RSP Service Plugin. This deletes the entire RSP configuration and disables the plugin.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click in the **RSP.servicelink** column on **Enable / Disable**.
4) Click **Reset to Default** followed by **OK**.
5) Click in the **RSP.servicelink** column on **Enable / Disable**.
6) Click on **Deactivate**.

7) Delete the device on the SIRA server (= OpenScape Business communication system).

NOTICE: You can find the device on the SIRA server via the MAC address. The MAC address of the OpenScape Business communication system can be found in the **Service Center** under **Inventory**.

25.16.1.5 How to Configure a PIN for Activating and Deactivating the RSP.servicelink Plugin

The PIN for activating and deactivating the RSP.servicelink plugin via a system telephone.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Enter the desired four-digit PIN in the **PIN** field.
4) Click **Save** followed by **OK**.

Next steps

The activation of the primary service plugin via a system phone occurs by entering the corresponding code (default code = *996), followed by the four-digit PIN.

The deactivation of the service plugins via a system phone occurs by entering the corresponding code (default code = #996), followed by the four-digit PIN.

25.16.2 Remote Access

Remote access can be used by authorized service technicians to access the OpenScape Business X communication systems remotely via an Internet connection. This ensures that support is available when solving administration tasks or performing troubleshooting.

You must enable remote access to activate remote access to the communication system. The following access method is possible:

Remote Access via Internet Connection

INFO: Remote access via an Internet connection presents a higher security risk.

To dial in via the Internet, the service technician needs a special port (**Port Number**) to access the communication system. Port number 10099 is specified

by default. When using an external router, port forwarding must be set up in the external router for this port number.

The port number must not be blocked by a possible firewall on the PC of the service technician. Port number selection should therefore be coordinated with the service technician.

The UC Booster Applications (e.g., UC Suite, Open Directory Service, Gate View) cannot be administered via this remote access.

You must disable remote access to block remote access to the communication system.

NOTICE: To prevent unauthorized access to the communication system, remote access must be turned off when completing the remote administration.

25.16.2.1 How to Enable Remote Access via ISDN

The **Remote Access** wizard can be used to provide authorized service technicians with access to the communication system via an ISDN connection.

Prerequisites

OpenScape Business X has an ISDN trunk connection.

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click on **Remote Access** to start the **Remote Access** wizard.
4) Activate the radio button **Remote access: on** to enable remote access.
5) Activate the radio button **Remote Access via: ISDN** to enable remote access via ISDN.
6) Enter the internal call number you want to use for remote access in the **Call No** field.
7) Enter the DID number you want to use for remote access in the **MSN/DID Number** field.
8) Click on **OK & Next** followed by **Finish**.

25.16.2.2 How to Configure PCs with Microsoft Windows Vista for Remote Access via ISDN

Prerequisites

The PC is equipped with an ISDN card and has an ISDN trunk connection.

An OpenScape Business X3/X5/X8 communication system with a point-to-point connection is to be accessed. The local area code and PABX number of the communication system are known.

Remote access via ISDN has been enabled. The dial-in number for remote access to the communication system is available.

The User Name and Password for accessing the communication system are known.

INFO: The following description applies to a PC with the Microsoft Windows Vista operating system The procedure for PCs with the Microsoft Windows XP operating system is analogous to the one described below.

Step by Step

1) Click **Start** in Windows Vista and select **Connect To**. The **Connect to a network** window appears.
2) Click on **Set up a connection or network**.
3) Click on the connection option **Connect to a workplace** and then on **Next**.
4) Click on **Dial directly**.
5) In the **Telephone number** field, enter the CO code (e.g., `0`), followed by the local area code (e.g., `089`), the PABX number (e.g., `12345678`) and the dial-in number (e.g., `666`).

   The complete entry for the example above would thus be:
   `008912345678666`
6) Enter a designation for this connection in the **Destination name** field.
7) Enable the check box **Don't connect now; just set it up so I can connect later**.
8) Click on **Next**.
9) Enter the user name for accessing the communication system in the **User name** field
10) and the password for accessing the communication system in the **Password** field.

NOTICE: The default user name and the default password for system access via the Manager E service tool are used as the default credentials for accessing the communication system.

---

11) Click on **Create**.
12) Click on **Connect now**.

This enables remote access to the communication system.

INFO: To deactivate the connection, click on **Start** > **Connect To**. Click on the designation of the connection defined in step 6 (**Destination name**) and then on **Disconnect**.

To activate the connection, click on the designation defined in step 6 (**Destination name**) and then on **Connect**.

25.16.2.3 How to Configure PCs with Microsoft Windows 7 for Remote Access via ISDN

Prerequisites

The PC is equipped with an ISDN card and has an ISDN trunk connection.

An OpenScape Business X3/X5/X8 communication system with a point-to-point connection is to be accessed. The local area code and PABX number of the communication system are known.

Remote access via ISDN has been enabled. The dial-in number for remote access to the communication system is available.

The User Name and Password for accessing the communication system are known.

INFO: The following description applies to a PC with the Microsoft Windows 7 operating system

---

Step by Step

1) Click in the **Start** menu of Windows 7 on **Control Panel**.
2) Click on **Network and Internet**.
3) Click on **Network and Sharing Center**.
4) Click on **Set up a connection or network**.
5) Click on the connection option **Connect to a workplace** and then on **Next**.
6) Click on **Dial directly**.
7) In the **Telephone number** field, enter the CO code (e.g., `0`), followed by the local area code (e.g., `089`), the PABX number (e.g., `12345678`) and the dial-in number (e.g., `666`).

   The complete entry for the example above would thus be: `008912345678666`
8) Enter a designation for this connection in the **Destination name** field.
9) Enable the check box **Don't connect now; just set it up so I can connect later**.
10) Click on **Next**.
11) Enter the user name for accessing the communication system in the **User name** field
12) and the password for accessing the communication system in the **Password** field.

NOTICE: The default user name and the default password for system access via the Manager E service tool are used as the default credentials for accessing the communication system.

---

13) Click on **Create**.
14) Click on **Connect now**. The message `Connection established` then appears.
15) Click on **Close**.

This enables remote access to the communication system.

INFO: To deactivate the connection, click on the **Networking** icon in the toolbar. Click on the designation of the connection defined in step 8 (**Destination name**) and then on **Disconnect**.

To activate the connection, click on the designation defined in step 8 (**Destination name**) and then on **Connect**.

25.16.2.4 How to Enable Remote Access via Internet Access with a Fixed IP Address

The **Remote Access** wizard can be used to provide authorized service technicians with access to the communication system via an Internet connection.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

You have a port number which can be used for Internet access to the communication system by the service technician. This port number must not be blocked by a possible firewall on the PC of the service technician.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click on **Remote Access** to start the **Remote Access** wizard.
4) Activate the radio button **Remote access: on** to enable remote access.
5) Enable the radio button **Remote Access via: Internet** to enable remote access via the Internet.
6) Enter the port number you want to use for remote access in the **Port Number** field.

   Port number 10099 is specified by default.
7) Click on **OK & Next**. The message `Remote Access has been activated ...` is displayed. This message includes the URL, via which the communication server can be accessed remotely using a web browser.
8) Click on **Finish**.

25.16.2.5 How to Enable Remote Access via Internet Access without a Fixed IP Address

The **Remote Access** wizard can be used to provide authorized service technicians with access to the communication system via an Internet connection.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

You have a port number which can be used for Internet access to the communication system by the service technician. This port number must not be blocked by a possible firewall on the PC of the service technician.

A DynDNS account is available.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click on **Remote Access** to start the **Remote Access** wizard.
4) Activate the radio button **Remote access: on** to enable remote access.
5) Enable the radio button **Remote Access via: Internet** to enable remote access via the Internet.
6) Enter the port number you want to use for remote access in the **Port Number** field.

   Port number 10099 is specified by default.
7) Click on **OK & Next** to accept the entries. The **Configure DynDNS-Account** window appears.
8) Enter the user name for your DynDNS account with the DynDNS provider in the **Login Name** field if this is not already displayed.
9) Enter the password of your DynDNS account with the DynDNS provider in the **Password** and **Retype Password** fields if this is not already displayed.
10) In the **Hostname** field, enter the host name assigned to you by the DynDNS provider, but without the domain name (e.g., `myhost`) if this is not already displayed.
11) Select your DynDNS provider in the **Domain name** drop-down list (e.g., `dyndns.org`) if this is not already displayed. Your complete domain name would then be `myhost.dyndns.org`, for example.
12) Click on **Connection test**. The **Test DynDNS Access** window appears.
13) Click on **OK**. The DynDNS access data is now transmitted to the provider. This takes about 10 seconds.
14) If the test was successful, the message `Remote Access has been activated ...` is displayed. This message includes the URL, via which the communication server can be accessed remotely using a web browser. Click on **Finish**.
15) If the test was successful, click **OK**. Notes on the possible causes of errors, if any, will appear in the subsequent **DynDNS Access** window. Click on **OK**. The **Configure DynDNS-Account** window appears. You can now check and correct the access data you had entered (steps 8 through 11) if required). Continue as described under step 12.

25.16.2.6 How to Disable Remote Access

The **Remote Access** wizard can also be used to disable remote access.

Prerequisites

You are logged on to the WBM with the **Advanced** profile.

Step by Step

1) Click on **Service Center** in the navigation bar.
2) Click on **Remote Access** in the navigation tree.
3) Click on **Remote Access** to start the **Remote Access** wizard. Shows whether remote access via the Internet and/or ISDN is enabled.
4) Activate the radio button **Remote access: off** to disable remote access.

5) Select the remote access option you want to disable:
   - If you want to disable remote access via the Internet, enable the **Remote Access via: Internet** radio button.
   - If you want to disable remote access via ISDN, enable the **Remote Access via: ISDN** radio button.
6) Click on **OK & Next**.
7) Click on **Back** if you also want to deactivate the second remote-access option. Repeat steps 4 through 6.
8) Click on **Finish**.

25.16.3 Online User

The Online User enables the remote control, verification and monitoring of OpenStage telephones via a Windows PC. The behavior of an OpenStage telephone is recreated via the Online User on the PC.

In order to communicate with an OpenStage phone, the phone software must have a so-called dongle key.

The following entries must be made via the Online User in order to access an OpenStage telephone:

- OpenStage phone type
- IP address of the OpenStage telephone
- Administrator password of the OpenStage telephone

Details on using the Online User can be obtained from the following documentation: *OpenStage HUSIM Phone Tester User Guide*. Access to this document is available via the intranet portal for technical product documentation at `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

The Manager E service tool provides online users for the remote control, testing and monitoring of OpenStage phones.

NOTICE: The gateway IP address reported by Online User is the same as system IP address. Gateway IP address is not the default-route IP address.

25.16.3.1 How to Start the Online User

Prerequisites

You are logged into the WBM with the **Expert** profile.

Step by Step

1) In the navigation bar, click on **Expert Mode**.
2) In the navigation tree, click on **Maintenance** > **Online User**. The login window of the Online User is displayed.
3) Select the model of the desired OpenStage telephone from the **Model** drop-down list.

4) Enter the IP address of the desired OpenStage telephone in the **Phone IP** field.
5) Enter the administrator password of the desired OpenStage telephone in the **Password** field. The default administrator password is `123456`.
6) Select the desired transport protocol in the **Protocol** drop-down list.
7) Select one of the following options for the Internet Protocol Version IPv:
   - If you want to use Internet Protocol Version 4, select the option **IPv4**.
   - If you want to use Internet Protocol Version 6, select the option **IPv6**.
8) Select the number of key modules in the **Number of Key Modules** drop-down list.
9) Click on **OK** to initiate access to the desired OpenStage telephone.

INFO: Details on the operation of the Online User can be found in the *OpenStage HUSIM Phone Tester User Guide*, which can be retrieved from `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

---

26 Migration

Open Scape Business V1, V2 systems and HiPath 3000 systems can be migrated/upgraded to OpenScape Business V3.

The following migration / upgrade scenarios are supported by OpenScape Business V3 software.

NOTICE: It is vital to delete active Unify Phone users prior to e.g. system migrations, to avoid critical discrepancies between the OpenScape Business database and the cloud database. More information can be found in the Unify Experts Wiki Unify Phone Whitepaper.

NOTICE: See also How to Remove or Delete Unify Phone Users on page 1141.

OpenScape Business X System including UC Booster Card or Booster Server

- Software Upgrade from OpenScape Business X V2 to V3 with “V2 Mainboard”
- Hardware/Software Migration from OpenScape Business X V2 to V3 with “V3 Mainboard”
- Hardware/Software Migration from OpenScape Business X V1 to V3 with “V3 Mainboard”
- Hardware/Software Migration from OpenScape Business X V3 with “V2 Mainboard” to V3 with “V3 Mainboard”

OpenScape Business S System

- Software Upgrade from OpenScape Business S V2 to V3

OpenScape Business Network

- Migration / Upgrade of an OpenScape Business network from V2 to V3

HiPath 3000 including OpenScape Office HX

- Hardware Migration HiPath 3000 including OpenScape Office HX

HiPath 500

- Hardware Migration HiPath 500 to OpenScape Business X1 V3

Depending on the source system, existing licenses can be transferred completely or partially. The same applies to the further use of peripheral modules and connected terminal devices.

Existing software support for OpenScape Business Systems will stay unchanged after the migration.

You can reduce the migration / upgrade efforts for the continued use of existing licenses, compared to an "offline" license transfer, by connecting the OpenScape Business System to the Unify Central License Server and using the **CLS Connect** feature .

Within this section, the following terms are used:

Migration	in case of Hardware and Software change
Upgrade	in case of a pure Software change
V2 mainboard	term used for the mainboard family introduced with OpenScape Business.
V3 mainboard	term used for the mainboard family that has been introduced with Software V3.

NOTICE: A prerequisite for all migration scenarios in order to upgrade from a V2 mainboard to a V3 mainboard system, is that the administrator has to upload the backup set via HTTPS device. Other devices such as Hard Disk, FTP or Network drive are not supported and will fail the migration process.

NOTICE: There are two valid migration paths depending on the software version of the OSBiz system. Either use a backup set from a V2 hardware system on the latest V2R7 bind, or use the same V3 software bind on both the V2 mainboard and V3 mainboard systems to ensure consistency in the database.

NOTICE: If an OpenScape Office V3 MX/LX system will be replaced with an OpenScape Business system, the last one must be ordered as a new system.

26.1 Software Upgrade for OpenScape Business X Systems

A Software upgrade of OpenScape Business X systems essentially involves replacing some of the SW components.

Before upgrading the software of an OpenScape Business X system, you must determine the current system configuration and the hardware/software and license components to be replaced, if applicable.

Table 31: OpenScape Business X Software Upgrade - Hardware/Software Checklist

Components	Replaced by
Hardware Components	
Software Components	
V2 Systems software on SDHC card	V3 System software (image from Software Download Server)
VPN on WAN in the system terminated	VPN in external router terminated
XMPP	No follow-on solution
myPortal Smart	myPortal @work

Components	Replaced by
License Components	
Licenses in license file	Transfer of the licenses into a new license file

26.1.1 Software Upgrade of OpenScape Business X V2 to OpenScape Business X V3

When you SW upgrade an OpenScape Business X model from software version V2 to V3, only the system software is replaced - the V2 mainboard and any existing UC booster card or booster server are retained. Existing licenses and the customer configuration are maintained. The existing software support will continue unchanged after the migration.

Before the software upgrade from version V2 to V3, if not already existing, you must set up a permanent access to the Unify License Server (via Internet) in the system and activate the function **CLS Connect**. This simplifies the license transfer and shortens the migration time considerably.

Prerequisites

For the SW upgrade and the transfer of the existing customer configuration, the system must be operated with the last released SW version V2R7 before the upgrade. If necessary, upgrade the system to the latest SW version. To do this, the system must have a valid Software Support status.

For the system SW upgrade from V2 to V3, depending on whether CLS Connect is used or not, the following item is required:

- OpenScape Business V3 SW Upgrade License (only when **CLS Connect** is not used)

Functional boundary conditions and restrictions

You can completely transfer existing licenses from the existing V2 mainboard to the V3 mainboard in the course of the migration. License transfer without activating the CLS Connect function requires the “SW Upgrade” license and a much more complex handling and time expenditure than using the CLS Connect function.

The customer configuration and customer data are automatically transferred from SW version V2 to V3 during the SW upgrade process.

The main technical steps of the SW upgrade are described in the following chapters. To retain the existing licenses a distinction regarding the handling is made between:

- SW Upgrade for permanent licensing with and without CLS Connect
- SW Upgrade with PayGo licensing

26.1.1.1 SW Upgrade of permanently licensed systems with CLS Connect

Perform the following upgrade steps in sequence.

Step by Step

1) Prepare the OpenScape Business System
   a) Upgrade the existing system to software version V2R7.
   b) Set up access to the Unify Central License Server (CLS) in the system and test the connection.
   c) Activate **CLS Connect** in the system.
2) Perform software upgrade
   a) Perform software upgrade to V3 via the OpenScape Business Assistant.
   b) System configuration is automatically transferred to V3.
   c) Existing licenses are taken over after V3.
3) Automatic generation of the license file by the central license server.
   After restarting the system, the system transfers the information that the existing licenses are operated with software version 3 to the CLS.

26.1.1.2 SW Upgrade of permanently licensed systems without CLS Connect

Perform the following upgrade steps in sequence.

Step by Step

1) Prepare the OpenScape Business System.
   a) Upgrade the existing system to SW version V2R7.
2) Create "Upgrade License File" for the V2 system at the Central License Server (CLS)
   a) Activate the "SW Upgrade License" for the existing system.
   b) Generate a new license file for the MAC address of the V2 mainboard
   c) Download the license file from CLS
3) Import and activate the license file in the OpenScape Business V2 system.
4) Perform SW upgrade.
   a) Perform SW Upgrade to V3 via the OpenScape Business Assistant.
   b) System configuration is automatically transferred to V3.
   c) Licenses existing in the system are transferred to V3
5) Reboot the system after SW upgrade.

26.1.1.3 SW Upgrade of PayGo licensed systems

Perform the following upgrade steps in sequence.

Step by Step

1) Prepare OpenScape Business System
   a) Upgrade the existing system to SW version V2R7.
2) Regenerate the license file on the central license server (CLS)
   a) Regenerate a new license file for the MAC address of the V2 mainboard.
   b) Download the license file from CLS.
3) Import and activate the new license file in the OpenScape Business V2 system.

4) SW Upgrade OpenScape Business SW
   a) Performing a SW upgrade to V3 via the OpenScape Business Assistant.
   b) System configuration is automatically transferred to V3.
   c) The system is ready for operation after restart.

26.2 Software Upgrade of UC Booster Server to OpenScape Business X V3

The SW upgrade from a UC Booster Server V2 to version V3 can be done in one step.

A SW upgrade from a UC Booster Server V1 to version V3 must be done in two steps. First upgrade from V1 to V2R7, then from V2R7 to V3.

26.2.1 How to Upgrade UC Business Booster Server V2 to V3

The SW Upgrade of the UC Booster Server from V2 to V3 is only necessary for OpenScape Business X systems with a V2 Mainboard. OpenScape Business X systems with V3 mainboards do not require a UC Booster Server any longer. In this case SW version V2.7 is required on the UC Booster Server to migrate customer configuration and licenses to the V3 mainboard.

Prerequisites

- Linux operating system must be checked and upgraded if necessary (see *technical Release note for OpenScape Business V3 system SW*)
- UC Booster Server is operated with the last released SW version V2R7 before the upgrade. If necessary, upgrade the system to the latest SW version.
- First update the OpenScape Business X system to which the UC Booster Server is connected to SW Version V3 including licensing according to description in Software Upgrade of OpenScape Business X V2 to OpenScape Business X V3 on page 1309
- UC Booster Server SW Image V3

Before a UC Booster Server SW upgrade, determine the current system configuration and the HW / SW and license components that may need to be replaced.

Table 32: OpenScape Business S Migration - HW/SW Checklist

Components	Replaced by
Hardware Components	
Server PC	Reuse is possible. HW Requirements must be checked for OpenScape Business S extensions.[10]
Software Components	

[10] The existing server PC HW can be used when the configuration of the UC Booster Server System remains unchanged after the SW upgrade. If expansions are planned after the SW upgrade, the hardware requirements may need to be adapted according to the specifications in *OpenScape Business S Installation Guide, chapter Prerequisites*.

Components	Replaced by
SLES 12 or SLES 15 Operating System	Reuse is possible. Eventually an upgrade to latest service pack is required[11]
XMPP	No follow-on solution
myPortal Smart	myPortal @work
License Components	
Licenses in license file (is part of the OpenScape Business X license file)	Transfer of the licenses into a new license file
CSTA application (via UC Booster card / server)	CSTA license for connecting external solutions (not required for UC Suite, TAPI 170 and TAPI 120)

The following describes the OpenScape Business SW Upgrade while keeping the SLES operating system.

Step by Step

1) Upgrade OpenScape Business X system to V3.
   See Software Upgrade of OpenScape Business X V2 to OpenScape Business X V3 on page 1309 for details.
2) Upgrade the UC Booster Server SW to V3
   Use the upgrade function within the OpenScape Business Assistant of the UC Booster Server to upgrade the V2R7 SW to the version V3 (see Updating the Communication System on page 1190).
3) Perform a data backup after SW upgrade
   Back up your V3 data (see Immediate Backup on page 1184)

26.3 Hardware/Software Migration of OpenScape Business X Systems to V3

When migrating OpenScape Business X systems, both HW, SW and license components are exchanged.

Before migrating a Business X system, determine the current system configuration and the HW / SW as well as license components to be replaced.

NOTICE: The OCCLA board with V3 system can go up to 60 (+16) MEB channels. Migration to the new board is restoring

11 The SLES operating system installed on the server PC can be adopted in case of a UC Booster Server SW upgrade. However, it should be upgraded to the last released service pack before the SW upgrade.

If Novell has discontinued SW support for the SLES version used, the customer must be informed and, if necessary, a SLES upgrade must be marketed.

The SLES upgrade may have to be performed in several steps to take over existing OpenScape Business S installations including the customer configuration and customer data. An existing SLES Update Key remains valid with a SLES Upgrade. However, it may have to be de-registered with Novell before the SLES upgrade and then re-registered for the new system.

the existing OCC configuration. If you want to take advantage of the additional MEB Channels, then you should reconfigure your system by using the appropriate wizards/WBM pages.

Modules that are present in slot 10 of OpenScape Business X5 wall systems cannot be operated in conjunction with V3 mainboards. These modules must be replaced by successor modules / solutions.

Table 33: OpenScape Business X Migration - HW/SW Checklist

Component	Replaced by
Hardware Components	
Existing “V2 mainboard”	V3 mainboard (basic or advanced, depending on configuration)
UC Booster card / server (with UC Suite)	Additional M.2 SSD
CMA module	CMAe module
EXMR module for external announcement devices	V3 Mainboard (Audio In jack on the front panel)
S0 interfaces on the V2 Mainboard	S0 terminal of S0 peripheral card
X5W cards for slot 10 • SLCN16 • SLA16N • SLA24N	Replaced by: • Cordless direct connect • SLAV16 • SLAV16 + SLAV8
Optipoint 500 phones	OpenScape Deskphone CP phones
Optipoint 400 phones	
Software Components	
V2 System SW on SDHC card	V3 System SW (Image from Software Download Server)
VPN on WAN in the system terminated	VPN in external router terminated
XMPP	No follow-on solution
myPortal Smart	myPortal @work
License Components	
Licenses in license file	Transfer of the licenses into a new license file
External CSTA applications (up to now license-free, because connected to UC Booster card / Server HW)	Separate CSTA license for connecting external solutions (not required for UC Suite, TAPI 170 and TAPI 120)

26.3.1 Migration from OpenScape Business X V2 to OpenScape Business X V3

When migrating an OpenScape Business X model from V2 to V3, the mainboard and the system software are replaced. Existing licenses and the customer configuration can be transferred. The existing software support is continued unchanged after the migration.

Before the migration, if not already existing, configure a permanent access to the Unify License Server (via Internet) in the system and activate the "CLS Connect" feature. This simplifies the license transfer and shortens the migration time considerably. The customer must be informed about the required access from the OpenScape Business System to the CLS.

Prerequisites

The system is operated with the last released SW version V2R7 before the upgrade. When necessary, upgrade the system to the latest SW version. To do this, the system must have a valid Software Support status.

For the migration from V2 to V3, depending on whether CLS Connect, UC Suite or external CSTA applications are used, the following items are required:

- V3 Mainboard
- V3 SW on M.2 SATA SSD data storage
- M.2 SSD 256 GB mass data storage (optional with UC Suite application)
- OpenScape Business V3 HW Migration License (if CLS Connect is not used)
- OpenScape Business CSTA License (optional)

Functional boundary conditions and restrictions

Existing licenses can be completely transferred from the existing V2 mainboard to the V3 mainboard during the migration. The license transfer without activating the CLS Connect function requires the "HW Migration" license and a much more complex handling and time expenditure than using the CLS Connect function.

The customer configuration and customer data are migrated from SW version V2 to V3 via a backup / restore process.

The main technical steps of the migration are described in the following topics. In order to retain the existing licenses a distinction regarding the handling is made between:

- SW Upgrade for permanent licensing with and without CLS Connect
- SW Upgrade with PayGo licensing

NOTICE: During the migration from V2 Mainboard to V3 Mainboard, the additional EVM ports are not additionally included in the SmartVM hunt group. This requires manual configuration, in the course of which one the COS restriction should be also made.

NOTICE: When performing a hardware migration from V2 hardware which is configured with non-default DSP IP address to a V3 hardware system, the DSP IP address will be reset to default value. After migration, the administrator has to manually

reconfigure the DSP IP address and also the FPGA IP address according to the specific customer needs.

26.3.1.1 How to Migrate to V3 Permanently Licensed Systems with CLS Connect

Perform the following migration steps in sequence.

Step by Step

1) Prepare the OpenScape Business System
   a) Upgrade the existing system to SW version V2R7
   b) Set up access to the Central License Server (CLS) in the system and test the connection
   c) Activate CLS Connect in the system

2) Generate license file at the central license server (CLS)
   a) Transfer the existing licenses from the MAC address of the V2 mainboard to the MAC address of the V3 mainboard using the **Regenerate** function
   b) Generate a new license file for the MAC address of the V3 mainboard

3) Backup the V2 system configuration and customer data.

4) Exchange mainboards
   a) Shut down the system and switch off all supply voltages
   b) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard
   c) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.
   d) Replace V2 Mainboard by V3 Mainboard in the system
   e) Switch on supply voltages again

      The system boots automatically.

5) Set basic system parameters within WBM after startup
   a) Set system date and time
   b) Set application package

      UC Smart for system without UC or with UC Smart

      UC Suite for systems with UC Suite

6) Restore the system configuration
   a) Restoring the backup using the restore function
   b) Importing the newly created license file

26.3.1.2 How to Migrate to V3 Permanently Licensed Systems without CLS Connect

Perform the following migration steps in sequence.

Step by Step

1) Prepare the OpenScape Business System
   a) Upgrade the existing system to SW version V2R7

2) Create "migration license file" for the V2 system at the central license server (CLS)
   a) Activate the "HW Migration License" for the existing system
   b) Generate a new license file for the MAC address of the V2 mainboard.
      For this, enter the MAC address of the V3 mainboard.
   c) Download the license file from CLS

3) Import the license file into the OpenScape Business V2 system

4) Take a note of the **Confirmation Code** displayed in the OpenScape Business Assistant

5) Generate a new license file for the V3 mainboard at the central license server (CLS)
   a) Create a new license file for the MAC address of the V3 mainboard at the CLS by regenerating the MAC address of the V2 mainboard and the previously noted confirmation code
   b) Search for the OpenScape Business System with the MAC address of the V3 mainboard in the CLS.
   c) Unlock the OpenScape Business System by entering and activating the Confirmation Code
   d) Regenerate the license file
   e) Download the newly generated license file from CLS

6) Backup the V2 system configuration and customer data.

7) Exchange mainboards
   a) Shut down the system and switch off all supply voltages
      a) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard
      b) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.
      c) Replace V2 Mainboard by V3 Mainboard in the system
   b) Switch on supply voltages again
      The system boots automatically.

8) Set basic system parameters within WBM after start-up
   a) Set system date and time
   b) Set application package
      UC Smart for system without UC or with UC Smart
      UC Suite for systems with UC Suite

9) Restore the system configuration
   a) Restore the backup using the restore function

10) Import manually the new license file into the V3 system after system start-up

26.3.1.3 How to Migrate to V3 PayGo Licensed Systems

Perform the following migration steps in sequence.

Step by Step

1) Prepare the OpenScape Business System
   a) Upgrade the existing system to SW version V2R7

2) Backup the V2 system configuration and customer data.

3) Regenerate the license file on the central license server (CLS)

a) Regenerate a new license file for the MAC address of the V3 mainboard

Transfer the existing licenses from the MAC address of the V2 mainboard to the MAC address of the V3 mainboard.

b) Download the new license file from the CLS

4) Exchange mainboards

a) Shut down the system and switch off all supply voltages

b) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard

c) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.

d) Replace V2 Mainboard by V3 Mainboard in the system

e) Switch on supply voltages again

The system boots automatically.

5) Set basic system parameters within WBM after startup

a) Set system date and time

b) Set application package

UC Smart for system without UC or with UC Smart

UC Suite for systems with UC Suite

6) Restore the system configuration

a) Restore the backup using the restore function

7) Import manually the new license file into the V3 system and activate the license file

26.4 Migration of an OpenScape Business X V3 System from V2 Mainboard to V3 Mainboard

In this scenario, the existing V2 mainboard of the OpenScape Business System and any UC Booster HW that can be present are replaced with a V3 mainboard. The system was previously upgraded to SW version V3, for example, in the course of the SW support.

Existing licenses and the customer configuration can be transferred. The existing software support service will continue unchanged after the migration.

A possibly existing UC Booster Card or a UC Booster Server is no longer necessary in connection with the V3 mainboard. An additional mass data storage is used on the V3 mainboard for this purpose.

In Table 33: OpenScape Business X Migration - HW/SW Checklist on page 1313 you can find information which components are substituted by using the V3 mainboard or are discontinued without substitution. A CSTA license is required for an existing connection of external CSTA applications. This does not apply to the connection of OpenScape TAPI 170 or TAPI 120.

Prerequisites

The system is operated with the last released SW version V2R7 before the upgrade. If necessary, upgrade the system to the latest SW version. To do this, the system must have a valid Software Support status.

For the migration, the following items are required, depending on whether CLS Connect, UC Suite or external CSTA applications are used:

- V3 Mainboard
- V3 SW on M.2 SATA SSD data storage
- M2 SSD 256 GB mass data storage (optional with UC Suite application)
- OpenScape Business V3 HW Migration License (optional)
- OpenScape Business CSTA License (optional)

Functional boundary conditions and restrictions

Existing licenses can be completely transferred from the existing V2 mainboard to the V3 mainboard in the course of the migration. The license transfer without activating the CLS Connect function requires the "HW Migration" license and a much more complex handling and time consuming than using the CLS Connect function.

The customer configuration and customer data are transferred via a backup / restore process.

The main technical steps of the migration are described in the following topics. In order to retain the existing licenses a distinction regarding the handling is made between:

- SW Upgrade for permanent licensing with and without CLS Connect
- SW Upgrade with PayGo licensing

NOTICE: During the migration from V2 Mainboard to V3 Mainboard, the additional EVM ports are not additionally included in the SmartVM hunt group. This requires manual configuration, in the course of which one the COS restriction should be also made.

Converting a KDS in the same software version to a different system type is not supported by Manager E. If you want to only use the KDS data you can try the following steps:

- Perform a full V2 mainboard to V3 mainboard system migration.
- Download the V3 mainboard system KDS with Manager E and store it locally.
- Reload the V3 mainboard system.
- Upload the previously stored V3 mainboard system KDS in your V3 mainboard system.

The V3 mainboard system will use the KDS database configuration and you can continue with the manual UC configuration.

NOTICE: Migrating the V2 mainboard system KDS to the V3 mainboard system is not supported, as the V2 mainboard database is not compatible with the V3 mainboard database.

26.4.1 How to Migrate to V3 Mainboard Permanently Licensed Systems with CLS Connect

Perform the following migration steps in sequence.

Step by Step

1) Prepare the OpenScape Business System
   a) Set up access to the Central License Server (CLS) in the system and test the connection
   b) Activate CLS Connect in the system

2) Generate license file at the central license server (CLS)
   a) Transfer the existing licenses from the MAC address of the V2 mainboard to the MAC address of the V3 mainboard using the **Regenerate** function
   b) Generate a new license file for the MAC address of the V3 mainboard

3) Backup the V3 system configuration and customer data.

4) Create a backup of the Booster Server configuration if necessary.

5) Exchange mainboards
   a) Shut down the system and switch off all power supplies
   b) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard
   c) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.
   d) Replace V2 Mainboard by V3 Mainboard in the system
   e) Switch on supply voltages again

      The system boots automatically.

6) Set basic system parameters within WBM after startup
   a) Set system date and time
   b) Set application package

      UC Smart for system without UC or with UC Smart

      UC Suite for systems with UC Suite

7) Restore the system configuration
   a) Import the newly created license file
   b) Restore the system backup and, if necessary, the Boster Server backup using the restore function

26.4.2 How to Migrate to V3 Mainboard Permanently Licensed Systems without CLS Connect

Perform the following migration steps in sequence.

Step by Step

1) Create "migration license file" for the existing V2 mainboard at the central license server (CLS)
   a) Activate the "HW Migration License" for the existing system
   b) Generate a new license file for the MAC address of the V2 mainboard
      For this, the MAC address of the V3 mainboard must be entered.
   c) Download the license file from CLS
2) Import the license file into the OpenScape Business System with V2 mainboard.
3) Take a note of the **Confirmation Code** displayed in the OpenScape Business Assistant
4) Generate a new license file for the V3 mainboard at the central license server (CLS)
   a) Create a new license file for the MAC address of the V3 mainboard at the CLS by regenerating the MAC address of the V2 mainboard and the previously noted confirmation code.
      a) Search for the OpenScape Business System with the MAC address of the V3 mainboard in the CLS.
      b) Unlock the OpenScape Business System by entering and activating the Confirmation Code
      c) Regenerate the license file
   b) Download the newly generated license file from CLS.
5) Backup the system configuration and customer data.
6) Exchange mainboards
   a) Shut down the system and switch off all supply voltages
   b) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard
   c) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.
   d) Replace V2 Mainboard by V3 Mainboard in the system
   e) Switch on supply voltages again
      The system boots automatically.
7) Set basic system parameters within WBM after startup
   a) Set system date and time
   b) Set application package
      UC Smart for system without UC or with UC Smart
      UC Suite for systems with UC Suite
8) Restore the system configuration after system startup
   a) Restore the backup using the restore function
9) Import manually the new license file into the V3 system after system startup.

26.4.3 How to Migrate to V3 Mainboard PayGo Licensed Systems

Perform the following migration steps in sequence.

Step by Step

1) Backup the system configuration and customer data.

2) Regenerate the license file on the central license server (CLS)
   a) Regenerate a new license file for the MAC address of the V3 mainboard
      Transfer the existing licenses from the MAC address of the V2 mainboard to the MAC address of the V3 mainboard.
   b) Download the new license file from the CLS

3) Exchange mainboards
   a) Shut down the system and switch off all supply voltages
   b) Use V3 data carrier and if necessary optional mass data storage on the V3 mainboard
   c) Remove the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the V3 mainboard.
   d) Replace V2 Mainboard by V3 Mainboard in the system
   e) Switch on supply voltages again
      The system boots automatically.

4) Set basic system parameters within WBM after startup
   a) Set system date and time
   b) Set application package
      UC Smart for system without UC or with UC Smart
      UC Suite for systems with UC Suite

5) Restore the system configuration after system startup
   a) Restore the backup using the restore function

6) Import manually the new license file into the V3 system and activate the license file

26.5 Software Upgrade of OpenScape Business S

Before an OpenScape Business S system software upgrade, determin the current system configuration and the HW / SW and license components that may need replacement.

Table 34: OpenScape Business S Migration - HW/SW Checklist

Components	Replaced by
Hardware Components	
Server PC	Reuse is possible. HW Requirements must be checked for OpenScape Business S extensions.[12]
Optipoint 400 phones	OpenScape Deskphone CP phones
Software Components	

[12] The existing server PC HW can be used if the configuration of the UC Booster Server System remains unchanged after the SW upgrade. If expansions are planned after the SW upgrade, the hardware requirements may need to be adapted according to the specifications in *OpenScape Business S Installation Guide, chapter Prerequisites*.

Components	Replaced by
SLES12 Operating System	Reuse is possible. Eventually an upgrade to latest service pack is required[13]
V2 System SW on SDHC card	V3 System SW (Image from Software Download Server)
XMPP	No follow-on solution
myPortal Smart	myPortal @work
License Components	
Licenses in license file	Transfer of the licenses into a new license file
CSTA application (via UC Booster card / server)	CSTA application (via UC Booster card / server)

26.5.1 Software Upgrade from OpenScape Business S V2 to OpenScape Business S V3

When upgrading an OpenScape Business S model from SW version V2 to V3, only the system SW is exchanged.

Existing licenses and the customer configuration are taken over. The existing software support will continue unchanged after the migration.

In this case, no separate order items are required for the System SW upgrade from V2 to V3.

That the SW version V3 no longer supports certain functions and hardware components. In Table 34: OpenScape Business S Migration - HW/SW Checklist on page 1321 you will find information about which components are substituted in version V3 and which components are omitted without substitution. This depends on the expansion of the customer system.

Prerequisites

The system operates with the last released SW version V2R7 before the upgrade. If necessary, upgrade the system to the latest SW version. To do this, the system must have a valid Software Support status.

[13] The SLES operating system installed on the server PC can be adopted in case of an OpenScape Business S / UC Booster Server SW upgrade. However, it should be upgraded to the last released service pack before the SW upgrade.

If Novell has discontinued SW support for the SLES version used, the customer must be informed and, if necessary, a SLES upgrade must be marketed.

The SLES upgrade may have to be performed in several steps to take over existing OpenScape Business S installations including the customer configuration and customer data. An existing SLES Update Key remains valid with a SLES Upgrade. However, it may have to be de-registered with Novell before the SLES upgrade and then re-registered for the new system.

The following describes the OpenScape Business SW Upgrade while keeping the SLES operating system.

Before the SW upgrade from version V2 to V3, setup a permanent access to the Unify license server (via the Internet) in the system and activate the **CLS Connect** function.

Functional Boundary Conditions and Restrictions

Existing licenses can only be taken over in the course of the SW upgrade if the CLS Connect function is activated.

The customer configuration and customer data are automatically transferred from SW version V2 to V3 during the SW upgrade process.

The main technical steps of the migration are described in the following chapters. To retain the existing licenses a distinction regarding the handling is made between:

- SW Upgrade for permanent licensing with and without CLS Connect
- SW Upgrade with PayGo licensing

Technical handling of the upgrade

The main technical steps of the upgrade are described below. A distinction is made between:

- Upgrade for permanent licensing with CLS Connect
- Upgrade with PayGo licensing

26.5.1.1 How to Upgrade to V3 Permanently Licensed Systems with CLS Connect

Perform the following migration steps.

Step by Step

1) Prepare the OpenScape Business V2 System
   a) Upgrade the existing system to SW version V2R7
   b) Set up access to the Central License Server (CLS) in the system and test the connection
   c) Activate CLS Connect in the V2 system

2) Prepare SLES operating system

   Upgrade the operating system to the service pack last released fro the SLES version used in connection with OpenScape Business S.

3) Upgrade OpenScape Business Software
   a) Execute the software upgrade to V3 via OpenScape Business Assistant.
   b) The system configuration is automatically transferred to V3.
   c) Existing licenses are transferred to V3.

4) License file is generated automatically by the central license server (CLS)
   a) After restarting the system, the system transfers the information that the existing licenses are operated with software version 3.
   b) The license server automatically generates a new license file with the V3 info and transfers it back to the system.

26.5.1.2 How to Upgrade to V3 PayGo Licensed Systems

Perform the following migration steps.

Step by Step

1) Prepare the OpenScape Business System
   a) Upgrade the existing system to SW version V2R7

2) Prepare SLES operating system
   Upgrade the operating system to the service pack last released fro the SLES version used in connection with OpenScape Business S.

3) Regenerate the license file on the central license server (CLS)
   a) Regenerate a new license file for the V2 system
   b) Download the new license file from the CLS

4) Import and activate the new license file in the OpenScape Business V2 system.

5) Upgrade OpenScape Business Software
   a) Execute the software upgrade to V3 via OpenScape Business Assistant.
   b) The system configuration is automatically transferred to V3.
   c) The system is ready for operation after reboot.

26.5.2 Software Upgrade from OpenScape Business S V2 to OpenScape Business S V3

Perform the following migration steps to upgrade an OpenScape Business S V1 system to an OpenScape Business S V2 system.

Prerequisites

Before performing the migration, check whether the hardware and software properties of the Linux server are appropriate for OpenScape Business S V2. An upgrade to the Linux server (for example, more available RAM) may be sufficient. The SLES 64 bit Linux operating system, that has been released for OpenScape Business V2 is a prerequisite. For the upgrade step to OpenScape Business SW version V3, the SLES 64 version that has been release for V3 is required.

If a new Linux server is required, the OpenScape Business V1 S communication software must be installed after installing Linux. A V1 data backup can then be transferred and you can continue with migration step 1.

Functional Boundary Conditions and Restrictions

When the system is upgraded from OpenScape Business V1 to OpenScape Business V2, then no ITSP activation/deactivation can be done in Internet Telephony wizard until a reset to LCR is done. Already configured ITSPs in OpenScape Business V1 will continue to work also in OpenScape Business V3 even without resetting the LCR. You can edit the already activated ITSP but not deactivate it. In order to make any activation/deactivation change in the wizard, reset the LCR. This is to reflect the necessary changes for the increase of ITSPs from 4 to 8. To reset LCR, go to **Expert Mode** > **LCR** > **LCR Flags** and click the **Reset LCR Data** flag.

Upgrade procedure

Perform the following upgrade steps.

1) **Update the OpenScape Business V1 software**

   Using the WBM, update the OpenScape Business V1 software to the version V1 R3.3 or higher (see Updating the Communication System on page 1190).

2) **Load the OpenScape Business V2 license file**

   Load the OpenScape Business V2 license file into the OpenScape Business V1 system and activate the licenses (see Activating Licenses (Standalone) on page 299).

   The license for the free SLES upgrades can still be used.

3) **Load the current OS Biz V2 software**

   Using the WBM, load the current OpenScape Business V2 software into the communication system. The V1 data is automatically converted to V3 data in the process (see Updating the Communication System on page 1190).

4) **Perform a data backup**

   Back up your V2 data (see Immediate Backup on page 1184).

26.6 OpenScape Business V2 Network Migration/Upgrade to V3

When migrating or upgrading an OpenScape Business network to V3, all nodes in the network must be upgraded to SW version V3. For the networking functions it is irrelevant whether the SW version V3 is operated on a OpenScape Business X system in the network with a V2 mainboard or with a V3 mainboard.

Upgrade each OpenScape Business node of the network separately. The components required for an upgrade are to be determined per node depending on the individual systems according to the descriptions in chapters Software Upgrade for OpenScape Business X Systems on page 1308, Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311, Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312 or Migration of an OpenScape Business X V3 System from V2 Mainboard to V3 Mainboard on page 1317.

The licenses for the nodes in the V2 network can be transferred to the V3 systems via the Central License Server. There are different procedures for systems with or without **CLS Connect** function. The “Pay as yo go” licensing procedure is not supported in the OpenScape Business network.

The effort required for transferring licenses with **CLS Connect** is significantly lower in a network than without the CLS Connect function.

IMPORTANT: Upgrade of the nodes in a network in the sequence as described for each scenario. It is essential, that all slave nodes are in operation with the software version V3 before the master node can be migrated or upgraded to software version V3.

During the network upgrade an heterogeneous network with V2 and V3 software will occur for a transitional period. During this time, the full functionality of the network's performance range cannot be guaranteed. In some scenarios the upgraded / migrated systems will operate in emergency mode only until the license file is updated by the master node.

OpenScape Business networks can be realized in various combinations regarding the use of OpenScape Business X and S systems and the licensing of the systems in the network. The most important steps for the migration or upgrade of an OpenScape Business network and their sequence are shown by means of typical combinations.

The description always assumes that a network license file exists in the Central License Server for the network, by means of which the master node supplies all slave nodes with license information.

- **Network consisting of OpenScape Business X Systems only**
  - Scenario 1: HW migration only in the master node, SW upgrade in all slave nodes
  - Scenario 2: SW upgrade for all OpenScape Business X nodes in the network
- **Network consisting of OpenScape Business S and OpenScape Business X systems**
  - Scenario 3: OpenScape Business S is master node and OpenScape Business X systems are slave nodes
    - Scenario 3a: SW upgrade in all OpenScape Business nodes of the network
    - Scenario 3b: SW upgrade in the OpenScape Business S master node, migration of the slave nodes

26.6.1 Scenario 1: Hardware Migration of Master node, Software Upgrade of Slave nodes

When migrating the network, a distinction must be made between the **CLS Connect** function and the license transfer procedure.

26.6.1.1 Migration/Upgrade with CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- The **CLS Connect** function is activated in the Master Node. CLS Connect does not have to be switched on in the Slave Nodes.

Step by Step

1) Upgrade all slave nodes to software version V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311)

a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.

b) Configuration and license information is kept.

The system is not operational after startup, due to invalid license file.

2) Generate a new network license file on the license sedrver.
   a) Regenerate the network license file for the Master node to the MAC address of the V3 mainboard
   b) Download new network license file from CLS
3) Migrate Master node to V3 mainboard (for details see Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312)
   a) Backup system configuration via WBM
   b) Exchange the mainboard
   c) Set date/time and application package via WBM
   d) Import and activate the new network license file via WBM.
   e) Restore the system configuration via WBM

   The license file is not overwritten in this case.
4) The master node automatically transfers the new license information to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.6.1.2 Migration/Upgrade without CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- Hardware Migration license for Master node is available
- Software Upgrade licenses are available for each Slave node

Step by Step

1) Generate new network license file on the license server
   a) Break down the network file at the CLS into individual license files
   b) Generate a license file for the master node

      Activate the hardware migration license for the master node
   c) Generate licese file for slave nodes

      Activate the software upgrade license for each individual slave node
   d) Merge the individual nodes license files to a new network license file
   e) Download the new network license file from CLS
2) Upgrade slave nodes to V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311)
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information are automatically transferred.

   The system is not operational after startup, due to invalid license file.

3) Migrate Master node to V3 (for details see Hardware/Software Migration of OpenScape Business X Systems to V3 on page 1312)
   a) Backup system configuration via WBM
   b) Switch the mainboard
   c) Set date/time and application package via WBM
   d) Import and activate the new network license file via WBM.
   e) Restore the system configuratin via WBM (license file is not overwritten in this case)
4) The master node automatically transfers the new license information to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.6.2 Scenario 2: Software Upgrade of all Systems in the Network to V3

When upgrading the network software, the use of **CLS Connect** function or not defines the procedure to be followed for transferring the license.

26.6.2.1 Software Upgrade with CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- The **CLS Connect** function is activated in the Master Node. CLS Connect does not have to be switched on in the Slave Nodes.

Step by Step

1) Migrate all slave nodes to software version V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311)
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) Configuration and license information is kept.

   The system is not operational after startup, due to invalid license file.
2) Upgrade Master node to V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information is retained.
   c) Restart the system.

3) Following steps are automatic (no manual intervention is required)
   a) Master node reports to CLS after startup with software version 3.
   b) CLS generates a new network license file.
   c) CLS transfers the new network license file to the master node.
   d) Maste node automatically transmits the new license infromation to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.6.2.2 Software Upgrade without CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- Software Upgrade licenses are available for each node

Step by Step

1) Generate new network license files on the license server
   a) Break down the network file at the CLS into individual license files
   b) Generate a license file for the master node
      Activate the software upgrade license for the master node
   c) Generate licese file for slave nodes
      Activate the software upgrade license for each individual slave node
   d) Merge the individual nodes license files to a new network license file
   e) Download the new network license file from CLS
2) Migrate all slave nodes to the V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311)
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information is retained.
   c) The system is not ready for operation after startup, due to invalid license file.

   The system is not operational after startup, due to invalid license file.
3) Upgrade Master node to V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information is retained.
   c) Import the network license file into the master node and activate the license file

4) The master node automatically transfers the new license information to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.6.3 Scenario 3a: Software Upgrade of all Nodes

In this scenario, the master node is an OpenScape Business S system, and the slave nodes are OpenScape Business X systems.

This scenario is identical to Scenario 2: Software Upgrade of all Systems in the Network to V3 on page 1328

26.6.4 Scenario 3b: Software Upgrade in the Master Node, Hardware Migration of the Slave Nodes

In this scenario the slave nodes are migrated to the V3 mainboard and SW version 3 by a HW/SW exchange. In the OpenScape Business S master system the SW is upgraded from V2 to V3. For the HW/SW upgrade of the network, the use of the CLS Connect function defines the license transfer procedure.

26.6.4.1 Migration / Upgrade with CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- The **CLS Connect** function is activated in the Master Node. CLS Connect does not have to be switched on in the Slave Nodes.
- V3 Mainboards including V3 software are available

Step by Step

1) Migrate all slave nodes to the V3 mainboard (for details see Hardware/ Software Migration of OpenScape Business X Systems to V3 on page 1312)
   a) Backup the system configuration via WBM
   b) Replace mainboards
   c) Set date/time and application package via WBM
   d) Restore the system configuration via WBM

   The system is not operational after startup, due to invalid license file.
2) Upgrade Master node to V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information is retained.
   c) Restart the system.

3) Following steps are automatic (no manual intervention is required)
   a) Master node reports to CLS after startup with software version 3.
   b) CLS generates a new network license file.
   c) CLS transfers the new network license file to the master node.
   d) Maste node automatically transmits the new license infromation to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.6.4.2 Migration / Upgrade without CLS Connect in the Master Node

Prerequisites

- All nodes in the network are operated with the last released SW version V2R7.x.
- At the Central License Server (CLS) there is a central network license file for the master node of the network.
- The software Upgrade license for the Master node is available
- Hardware Migration licenses are available for each slave node
- V3 Mainboards including V3 software are available

Step by Step

1) Generate a new network license file on the license server
   a) Break down the network file at the CLS into individual license files
   b) Generate a license file for the master node
      Activate the software upgrade license for the master node
   c) Generate licese file for slave nodes
      Activate the hardware migration license for each slave node
   d) Merge the individual nodes license files to a new network license file
   e) Download the new network license file from CLS
2) Migrate all slave nodes to the V3 mainboard (for details see Hardware/ Software Migration of OpenScape Business X Systems to V3 on page 1312)
   a) Backup the system configuration via WBM
   b) Replace mainboards
   c) Set date/time and application package via WBM
   d) Restore the system configuration via WBM

   The system is not operational after startup, due to invalid license file.
3) Upgrade Master node to V3 (for details see Software Upgrade for OpenScape Business X Systems on page 1308 or Software Upgrade of UC Booster Server to OpenScape Business X V3 on page 1311
   a) Import V3 software via OpenScape Business Assistant (WBM) and upgrade the system.
   b) The configuration and license information is retained.
   c) Import the network license file into the master node and activate the license file

4) The master node automatically transfers the new license information to the slave nodes.

NOTICE: This transmision of licenses to slave nodes may take up to 15 minutes.

26.7 Migrating from HiPath 3000 to OpenScape Business V3

This section describes the technical migration of HiPath 3000 / HiPath 500 V9 standalone systems and HiPath 3000 internetworks to OpenScape Business V3 with V3 mainboards.

When migrating from HiPath 3000 systems to OpenScape Business X V3 with V3 mainboards, depending on the hardware configuration, part of the hardware equipment of the system and the connected terminals / clients can be transferred.

Before migrating a HiPath 3000, the current system configuration and the HW / SW as well as license components to be replaced, if any, must be determined by subsequent checks.

General Checks

- **Function compatibility check**

  Please inform yourself about which features are longer supported or have changed as compared to HiPath 3000 V9. Chapter HiPath 3000 Changed/ Dropped Features and Interfaces on page 1355 lists the HiPath 3000 features that are no longer supported in OpenScape Business or have been replaced by newer features.
- **Software version check**

  The system must be operated under SW version V9 before migration. Systems with SW version smaller than V9 must be upgraded to SW version V9 and put into operation before migration.
- **Protective earthing check**

  For all OpenScape Business X communications systems, protective grounding via an additional grounding conductor is mandatory!

Hardware compatibility check

For technical reasons, some modules and devices cannot be used in the OpenScape Business X systems. When migrating from HiPath 3000 V9 to OpenScape Business V3 these modules and terminals must be removed. If required, use the respective successor types instead. 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*.

- **Power Supply**

  OpenScape Business 33xx / 35xx can be operated with UPSC-D / DR or OCPSM power supply. Any remaining PSU power supplies must be replaced with OCPSM. Suitable PSU upgrade kits are available.

- **Peripheral components**

  Please check whether the existing hardware can still be used. No longer supported modules or end devices must be removed and replaced by successors if necessary.
- **Backplane check**

  In HiPath 3550 systems, slot 10 of the backplane is no longer addressed by the V3 mainboard. Existing peripheral modules that use this slot cannot be operated in OpenScape Business.
- **Phone device check**

  OpenScape Business V3 systems with V3 mainboards support analog, ISDN, SIP and OpenStage or OpenScape Deskphone IP / CP devices. Existing Optiset E, Optipoint 4xx and Optipoint 5xx devices must be replaced.
- **Housing check**

  In migrated HiPath 33xx/35xx systems, the housing caps may have to be replaced and fan units installed if necessary.

  Corresponding delivery items are available.

Other checks

- **Call number plan for networked systems**

  With pure voice networking, open and closed numbering is possible. When using UC Suite, closed numbering is required in the network (network-wide UC functionality).

26.7.1 Migration of HiPath 33xx, 35xx, 3800 to OpenScape Business X3/X5/X8 V3

When migrating a HiPath 33xx, 35xx or 3800 system to OpenScape Business X V3, the mainboard, the determined peripheral groups and end devices as well as the system SW are replaced. Existing licenses can be migrated with an Upgrade License. The system configuration can be transferred. After migration, the OpenScape Business V3 system has a software support of 3 years.

For the migration from HiPath 3000 V9 to OpenScape Business V3 the following items are required in principle:

- V3 Mainboard
- V3 SW on SSD data storage
- M2 SSD 256 GB mass data storage (optional with UC Suite application)
- OpenScape Business Upgrade HiPath 3000 V9 (license migration), or
- OpenScape Business Upgrade HiPath 3000 V8 (license migration), or
- OpenScape Business Upgrade HiPath 3000 V7 (license migration)
- OpenScape Business CSTA License (optional)

If necessary, further hardware components and licenses must be ordered in addition. This depends on the configuration of the customer system.

In *OpenScape Business X3/X5/X8 Service Documentation* on section *Not Supported HW Components* you will find information on which components are substituted in version V3 or are discontinued without substitution. Please note that a CSTA license is required for an existing connection of external CSTA

applications. This does not apply to the connection of OpenScape Business TAPI 170 or TAPI 120.

Prerequisites

All HW / SW components have been checked for reusability.

All new HW / SW components are available

An upgrade license for upgrading from HiPath 3000 V7, V8 or V9 to OpenScape Business V3 has been ordered and the LAC of the upgrade license is available to retrieve the new license from the license server.

The system has been updated to latest SW version V9 for the technical SW migration and the transfer of the existing customer configuration.

The latest version of the Manager E is used

Determining the OpenScape Business licenses during the migration

The licenses existing in HiPath 3000 systems can be transferred to the OpenScape Business V3 system by activating the “OpenScape Business Upgrade HiPath 3000 (V7, V8 or V9)” license in the central license server. During the license transfer a new license file for the OpenScape Business V3 system is created with the following licenses.

Table 35: HiPath 3000 License Migration

HP 3000 License	OpenScape Business License	Remarks
	Basic license	Newly created incl. 3 years SW support
	OpenDirectory Base license	Newly created
	Web Collaboration Connector license	Newly created
	TDM user license	Number calculated from system configuration[14]
IP-Subscriber (ComScendo)	IP User License	1:1 transfer from HP 3000 license file
	TDM User Licenser	calculated from system configuration[14]
S2M Channels	IP/S2M/TI Trunk licenses	1:1 transfer from HP 3000 license file
Mobility Entry	Mobility User licenses	1:1 transfer from HP 3000 license file

[14] Determined in the course of the technical conversion description see below.

Determination of the TDM user licenses within the license file

During the technical conversion of the HiPath 3000 system configuration, the number of active TDM subscribers is determined by the Manager E tool and written to an "inventory (XML) file".

The number of TDM user licenses is determined as follows:

- 1x TDM user license per active UP0 port - phone (master/slave) ready, phone number available
- 1x TDM User License per registered DECT phone - phone number available
- 1x TDM user license per active a/b port (phone number) for plugged modules
- 1x TDM user license per active S0 port (MSN phone number) for active modules

The TDM user license migration itself is performed offline at the CLS via the XML inventory file.

The central license server checks whether a license file exists for the MAC address of the HiPath 3000 mainboard.

If a license file is available, the license migration is performed on the basis of this license file and the information in the "inventory file".

If no license file is available, the OpenScape Business upgrade is performed on the basis of the information in the "Inventory (XML) file

Depending on the available Upgrade License (V7, V8 or V9) the following percentage of the determined TDM users are taken over to OpenScape Business.

- Upgrade from HiPath 3000 V4 or older to OpenScape Business V3:

  No TDM users are calculated for cheaper / free of charge OpenScape Business upgrade licenses
- Upgrade from HiPath 3000 V5, V6 or V7 to OpenScape Business V3:

  70% of TDM users are calculated for cheaper / free of charge OpenScape Business upgrade licenses
- Upgrade from HiPath 3000 V8 to OpenScape Business V3:

  80% of TDM users are calculated for cheaper / free of charge OpenScape Business upgrade licenses
- Upgrade from HiPath 3000 V9 OpenScape Business V3:

  100% of TDM users are calculated for cheaper / free of charge OpenScape Business upgrade licenses.

Functional boundary conditions and restrictions

- The license migration can be done to V3 only. A license migration to V2 is not supported by Manager E.
- The license migration of a HiPath 3000 system (mainboard) can only be performed once, and the mainboard is blocked for further actions at the CLS after the migration.
- To migrate S2M lines and ComScendo subscribers, a HiPath 3000 license file must be available on the central license server.
- The TDM user licenses generated during the migration cannot be transferred to other systems or to a CLS account.

- User licenses and UC user-oriented licenses are permanently assigned to the subscribers in OpenScape Business. Please note that for myAgent and myAttendant users the sufficient number of licenses is available. In OpenScape Business, changes of the presence status for other users by myAgent users are bound to the myAttendant license. These must be ordered separately.
- The Deskshare User (IP Mobility) feature requires a license in OpenScape Business as opposed to HiPath 3000. Additional IP user licenses must be available and assigned to the "Deskshare Users" within the OpenScape Business Assistant licensing dialog.
- No license migration is performed for the following products and features:
  - HG1500 B-channels: The board is dropped, since the functionality is integrated on the new mainboard.
  - optiClient Attendant V8: does not run on OpenScape Business.

    Follow-up product: OpenScape Business Attendant
  - optiClient BLF V1/V2: does not run on OpenScape Business.

    Follow-up product: OpenScape Business BLF
  - HiPath TAPI 120/170 V2: does not run on OpenScape Business.

    Follow-up product: OpenScape Business TAPI 120/170
  - Entry VoiceMail: The module is dropped, since it is integrated on the new mainboard

    Follow up product: Smart Voicemail
  - myPortal entry web services communications clients on the plug PC.
  - Base stations: licenses for base stations are no longer required.
  - ITSP trunk access: licenses must be purchased to use ITSP channels for Internet telephony in OpenScape Business.
  - As in the past, no licenses are required for S0, Analog and CAS trunks.
  - For networking and the connection of external systems via tie lines, one network license per node must be purchased in OpenScape Business.

Technical handling

Perform the following migration steps in sequence:

1) Download the HiPath 3000 Customer Data Base (CDB) from the system

Download the current HiPath 3000 CDB from the HiPath 3000 system using the latest version of Manager E.

2) Record the HG1500 settings (optional)

If one or more HG1500 boards are plugged in, you must note the HG1500 settings that were changed with respect to the default settings using the HG1500 WBM:

- IP Routing
- PSTN Routing
- IP Firewall
- MAC Firewall
- Application Firewall
- IP Accounting
- IP Mapping
- SNMP

3) **Convert the HiPath 3000 CDB**

   Convert the current HiPath 3000 CDB to the OpenScape Business V3 CDB using the latest version of Manager E.

4) **Swap out the hardware**

   Replace the old HiPath 3000 mainboard with the new OpenScape Business V3 mainboard. Remove all HG1500 boards and all boards and sub-boards that are no longer supported. All OpenScape Business communication systems must be grounded with an additional ground wire.

5) **Perform the initial installation**

   Configure the communication system via the WBM with the **Initial installation** wizard. Note that the HG1500 settings you recorded earlier should also be taken into account here.

6) **Load the converted CDB**

   Load the converted CDB into the OpenScape Business V2 system using the latest version of Manager E. The OpenScape Business system will then restart automatically.

7) **Generate new license file at the CLS**

   Generate a new license file at the CLS with the LAC of the upgrade license, the configuration file (XML file) and the locking ID of OpenScape Business.

8) **Activate and assign licenses**

   License the OpenScape Business communication system within 30 days with the help of the license file.

9) **Reset LCR entries**

   If required, you can reset the configured LCR entries in the HiPath 3000 system (for example, dial plans, routing tables, dial rules) to the default entries of OpenScape Business. This setting can be found in the WBM in the **Basic Installation** wizard.

26.7.1.1 How to Load the CDB from HiPath 3000

Prerequisites

A HiPath 3000 communication system (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 and HiPath 3800) is available.

All phones are connected and active.

The latest version of Manager E is installed on the admin PC.

The admin PC is connected to the HiPath 3000 communication system.

Step by Step

1) Log into Manager E at the admin PC.
2) Click on **File** > **Transmit** in the menu bar.
3) Click on the **Communications** tab.
4) Select the appropriate option in the **Access** area, depending on the type of connection from the admin PC to the communication system.
5) Enable the radio button **Read/write CDB** and click on **System** > **PC**.
6) Click on **OK**. The CDB is transferred from HiPath 3000 to Manager E.
7) After the successful transfer, click **OK** and then on **Close**.

8) Click in the menu bar on **File** > **Save customer database as** and save the CDB on the admin PC in a folder of your choice.

Next steps

How Read out the HG1500 Settings on page 1338

26.7.1.2 How Read out the HG1500 Settings

Prerequisites

One or more HG1500 boards are inserted.

You are logged on to Manager E.

Step by Step

1) In Manager E, click in the System view on the HG1500 entry. The WBM of the HG1500 opens.
2) Make a note of the settings that have been changed from their default settings. The HG1500 settings are not transferred during the conversion of the CDB and must be entered again in the WBM at the initial startup of OpenScape Business.

Next steps

How to Convert the HiPath 3000 CDB on page 1338

26.7.1.3 How to Convert the HiPath 3000 CDB

Prerequisites

HiPath 3000 communication system (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 and HiPath 3800) is available.

The admin PC is connected to the HiPath 3000 communication system.

Step by Step

1) Click on **File** > **Convert customer database** in the menu bar.
2) Select the CDB previously stored on the admin PC and click **OK**.
3) Enter your **Name** and your **Contract number** as your customer data and click **Next**.
4) Select **OpenScape Business V2** as the **Version** and click **Next**.
5) Click **OK** to confirm the unsupported boards advisory messages.
6) Click **Yes** to confirm the window which informs you about the number of TDM users to perform the migration and proceed with the migration.

   The number of TDM user which will be migrated is calculated automatically.
7) Click **Next** to confirm the window which informs you about which boards are plugged.
8) Click in the menu bar on **File** > **Save customer database as** and save the CDB under a different name on the admin PC in a folder of your choice.
9) Close Manager E.

Next steps

How to Replace the HiPath 3300/3500 Hardware on page 1339 or

How to Replace the HiPath 3350/3550 Hardware on page 1340 or

How to Replace the Hardware for HiPath 3800 on page 1341

26.7.1.4 How to Replace the HiPath 3300/3500 Hardware

Prerequisites

A HiPath 3000 communication system (HiPath 3300 or HiPath 3500, rack-mount) is up and running.

OpenScape Business V3 Mainboard (OCCMRA or OCCMRB).

WARNING:

Risk of electric shock through contact with live wires

Make sure that a separate protective ground wire with the required minimum cross section is available for the communication system (see Service Documentation, Hardware Installation).

Step by Step

1) Switch off the HiPath 3000 system and disconnect the system's power plug.
2) Unplug all connectors (such as analog stations, ISDN lines, etc.) from the mainboard.
3) Loosen the two locking screws in the front panel of the mainboard.
4) Pry the mainboard loose from the backplane with two board wrenches (C39165-A7027-C26).
5) Using both hands, carefully slide out the HiPath 3000 mainboard horizontally from the board shelf and place it on a flat, grounded conductive surface.
6) Remove any existing HG1500 boards from the housing. The freed HG1500 slots can be used for additional boards.
7) If necessary, remove any boards that are no longer supported from the housing. The freed slots can be used for additional boards.
8) Remove all subboards inserted into the HiPath 3000 mainboard and plug them (if still needed and supported) into the OpenScape Business V3 mainboard.
9) Plug the M.2 SATA SSD with system SW and optional M.2 NVMe SDD on the V3 mainboard.
10) Plug optional modules such as OCCBH or OCCBL
11) Using both hands, carefully slide the OCCMRA or OCCMRB mainboard horizontally into the same slot in which the HiPath 3000 mainboard was previously located.
12) Connect optional modules such as STRBR to V3 mainboard.

13) Reconnect all connectors on the mainboard (such as analog stations, ISDN lines, etc.).

NOTICE: If more than 2 analog a/b ports were used in HiPath 3300 or 3500, 1 or 2 Y-adapter cables will be required in OpenScape Business. Up to 4 a/b ports can be connected through the 2 physical RJ11 sockets. Due to space constraints, the new mainboard has only 2 RJ11 sockets through which the 4 a/b stations must be connected.

14) Make sure that your communication system is properly connected to the ground wire.

15) Reconnect the system's power plug and power up the system.

Next steps

How to Perform the Initial Installation on page 1342

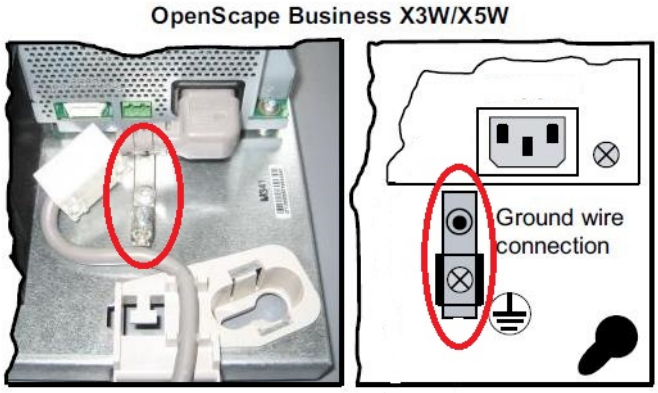
26.7.1.5 How to Replace the HiPath 3350/3550 Hardware

Prerequisites

A HiPath 3000 communication system (HiPath 3350 or HiPath 3550, wall-mount) is up and running.

OpenScape Business Mainboard (OCCMA or OCCMB).

In case of a migration from HiPath 3350 / 3550 to OpenScape Business X3W/X5W the protection ground terminal hast to be installed as shown in figure below. Afterwards the protection ground wire has to be connected as described within OpenScape Business V2, OpenScape Business X3/X5/X8, Installation Guide.



WARNING:

Risk of electric shock through contact with live wires

Make sure that a separate protective ground wire with the required minimum cross section is available for the communication system (see Service Documentation, Hardware Installation).

Step by Step

1) Switch off the HiPath 3000 system and disconnect the system's power plug.
2) Unlatch the housing and remove it.
3) Remove the cover.
4) Unplug all edge connectors (such as analog stations, ISDN lines, etc.) from the mainboard.
5) Remove the board latch.
6) Using both hands, carefully remove the HiPath mainboard from the board shelf and place it on a flat, grounded conductive surface.
7) Remove any existing HG1500 boards from the housing. The freed HG1500 slots can be used for additional boards.
8) If necessary, remove any boards that are no longer supported from the housing. The freed slots can be used for additional boards.
9) Remove all subboards inserted into the HiPath 3000 mainboard and plug them (if still needed and supported) into the OpenScape Business mainboard.
10) Plug the M.2 SATA SSD with system SW and optional M.2 NVMe SSD on the V3 mainboard.
11) Plug optional modules such as OCCBH or OCCBL.
12) Carefully insert the OpenScape Business OCCMA or OCCMB mainboard into the same slot in which the HiPath 3000 mainboard was previously located.
13) Connect optional modules such as STRBR to V3 mainboard.
14) Reconnect all edge connectors on the mainboard (such as analog stations, ISDN lines, etc.). Note that the connectors for ISDN lines must first be passed through the hole of the new board latch.
15) Secure the new board latch.
16) Make sure that your communication system is properly connected to the ground wire.
17) Put the housing back on and latch it.
18) Reconnect the system's power plug and power up the system.

Next steps

How to Perform the Initial Installation on page 1342

26.7.1.6 How to Replace the Hardware for HiPath 3800

Prerequisites

A HiPath 3800 communication system is up and running.

OpenScape Business Mainboard OCCLA.

WARNING:

Risk of electric shock through contact with live wires

Make sure that a separate protective ground wire with the required minimum cross section is available for the communication system (see Service Documentation, Hardware Installation).

Step by Step

1) Switch off the HiPath 3000 system and disconnect the system's power plug.
2) Unplug all connectors from the mainboard.
3) Using both hands, carefully slide out the HiPath 3000 mainboard from the board shelf and place it on a flat, grounded conductive surface.
4) Pull out any existing HG1500 boards from the board shelf. The freed HG1500 slots can be used for additional boards.
5) If present, remove any boards that are no longer supported from the board shelf. The freed slots can be used for additional boards.
6) Remove all subboards inserted into the HiPath 3000 mainboard and plug them (if still needed and supported) into the OpenScape Business mainboard.
7) Plug the M.2 SATA SSD with system SW and optional M.2 NVMe SDD on the V3 mainboard.
8) Plug optional modules such as OCCBH or OCCBL.
9) Carefully insert the OpenScape Business OCCLA mainboard into the same slot in which the HiPath 3000 mainboard was previously located.
10) Plug all connectors back into the mainboard.
11) Make sure that your communication system is properly connected to the ground wire.
12) Reconnect the system's power plug and power up the system.

Next steps

How to Perform the Initial Installation on page 1342

26.7.1.7 How to Perform the Initial Installation

The initial installation of the communication system is described in Integration into the Customer LAN).

The initial installation includes the configuration of the system's IP address, the DHCP settings and the country and time settings.

If an HG 1500 was installed together with the HiPath 3000, the IP address of the HG 1500 should be entered as the IP address of the OpenScape Business system during the initial installation.

After the initial installation has been completed successfully, the communication system performs a restart.

Next steps

How to Load the Converted CDB into the New System on page 1343

26.7.1.8 How to Load the Converted CDB into the New System

Prerequisites

The hardware has been replaced.

The admin PC is connected to the OpenScape Business communication system (via the LAN interface).

The admin PC is configured to receive the IP address and the subnet mask from the OpenScape Business DHCP server.

Step by Step

1) Log into Manager E at the admin PC.
2) Click on **File** > **Open customer database** in the menu bar.
3) Navigate to the location of the converted OpenScape Business CDB and click **OK**.
4) Confirm the message with **OK**.
5) Click on **File** > **Transmit** in the menu bar.
6) Click on the **Communications** tab.
7) Enable the **IP - HiPath** option in the **Access** area and enter the IP address of the OpenScape Business communication system in the IP address field. Default: `192.168.1.2`.
8) Enable the **Security** radio button.
9) Click on **Change Password**.
10) Enter the old and the new password and confirm with **OK**.
11) Enable the radio button **Read/write CDB**.
12) Enable the **Call Charges** and **Hardware** check boxes and click on **PC** > **system**.
13) Click **OK**. Manager E transfers the CDB to the system.
14) After successful transfer of the CDB, click **OK** and then on **Close**.
15) Exit Manager E. The system automatically performs a restart.

Next steps

How to Generate a New License File on page 1343

26.7.1.9 How to Generate a New License File

Prerequisites

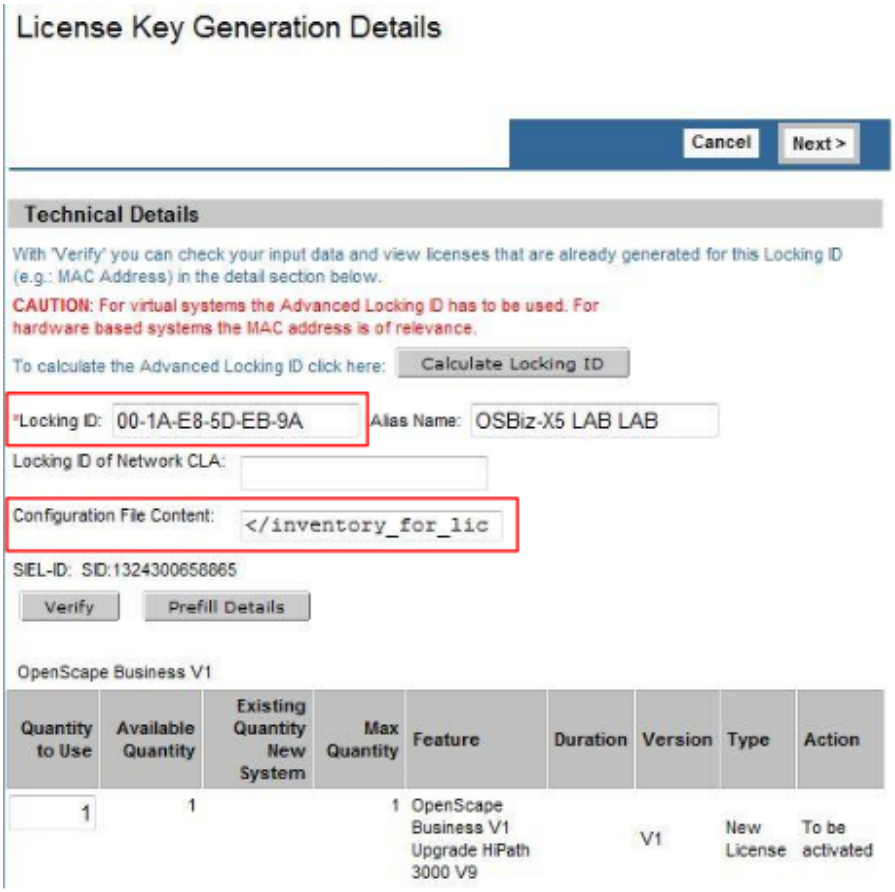
The LAC of the upgrade license is available.

The registration data of the customer is available.

Step by Step

1) Log into the WBM with the **Advanced** profile.
2) Click on **License Management** in the navigation bar.

3) Make a note of the locking ID of OpenScape Business, which appears above the table.
4) In the navigation tree, click on **Registration**.
5) Enter your data and click **OK & Next**.
6) Click **Export data**. A configuration file (XML file) is generated with the registration data and inventory information, including the number of connected TDM stations.
7) Save the configuration file in a directory of your choice.
8) Log into the CLS with the user name and password.
9) Click on **License** > **Generate License Key** in the menu tree.
10) Enter the LAC of the upgrade license under **LAC** and click **Generate Key**.
11) Select the feature **OpenScape Business V2 Update HiPath 3000** and click again on **Generate Key**.



12) Enter the Locking the ID of OpenScape Business in the **Locking ID** field.
13) Open the configuration file with a text editor (e.g., Notepad) and copy the entire contents of the configuration file into the **Configuration File Content** field.
14) Click **Next** and follow the instructions to generate a new license file.

NOTICE: The license migration procedure can only be performed once at the CLS. Consequently, please make sure that all the details are accurate!

---

15) Save the new license file in a directory of your choice.

Next steps

How to Activate a License File Offline on page 1345

26.7.1.10 How to Activate a License File Offline

Offline license activation is described in the chapter How to Activate Licenses Offline (Standalone).

Next steps

How to Assign Licenses on page 1345

26.7.1.11 How to Assign Licenses

The license assignment is described in Assigning Licenses (Standalone) on page 301.

26.7.1.12 How to Reset the LCR Entries

The basic installation of the communication system is described in Basic Configuration on page 150).

The basic installation includes the configuration of the system call number and the stations as well as access to the Internet and Internet telephony.

In the **Basic Installation** wizard, in the **Central Functions for Stations** window, you will find an additional radio button to **Delete the configured LCR data and initialize the LCR with default data**. This radio button appears only if a converted CDB was previously loaded into the system. If this radio button is selected, the configured LCR entries in the HiPath 3000 system will be deleted and replaced by the default entries of the OpenScape Business system.

Related concepts

Station Data on page 153

26.7.2 Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V3 with V3 Mainboard

When migrating HiPath 3000 systems with a connected OpenScape Office HX Server, the external server is not required. Its function is taken over by the corresponding V3 mainboard of the OpenScape Business X System.

The HiPath 3000 system is migrated as described in Migration of HiPath 33xx, 35xx, 3800 to OpenScape Business X3/X5/X8 V3 on page 1333.

OpenScape Office HX licenses are part of the HiPath 3000 license file. Therefore, they are also transferred to OpenScape Business licenses in the course of the HiPath 3000 license migration.

Requirements

To migrate OpenScape Business HX licenses, a HiPath 3000 license file must be available on the central license server.

For the HiPath 3000 licenses the license migration is performed as shown in Table 35: HiPath 3000 License Migration on page 1334. The following applies to the OpenScape Office HX license migration:

Table 36: OpenScape Office HX License Migration

OpenScape Office HX License	OpenScape Business License	Remarks
Per Basic license	1x AutoAttendant license	
Per OpenScape Office Standard User:	1x UC User 1x Voicemail User 1x Fax User	Applies to Standard User Licenses in the HX Basic Licenses 5/10 as well as to Single User Licenses
OpenScape Office HX Voicemail License	500 x Voicemail User	
myPortal for Outlook	Groupware User	Number as in the license file
myAttendant	myAttendant	Number as in the license file
myAgent	myAgent User	Number as in the license file
Contact Center Fax	Contact Center Fax User	Number as in the license file
Contact Center E-Mail	Contact Center E-Mail User	Number as in the license file
myReports	myReports	Number as in the license file
Application Launcher	Application Launcher	Number as in the license file
OpenDirectory Connector	OpenDirectory Connector	Number as in the license file

Functional boundary conditions and restrictions

The license migration can only be done to V3. A license migration to V2 is not supported by Manager E.

The license migration can only be performed once.

User licenses and UC user-oriented licenses are permanently assigned to the users in OpenScape Business. Please note that for myAgent and myAttendant users the sufficient number of licenses is available.

In OpenScape Business, changes of the presence status for other users by myAgent users are bound to the myAttendant license. These must be ordered separately.

It is not possible to transfer announcements, pictures, voicemails, fax, journal, contact center data, subscriber configuration, profiles, external directory, schedules from OpenScape Office HX to OpenScape Business V3 with V3 mainboard.

26.7.3 Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V3 with UC Booster Server

The Migration has to be done in two steps. In a first step the systems are migrated to V2. In a subsequent step the systems are migrated to V3.

This migration scenario should only be performed in case that customer data within the OpenScape Office HX server needs to be kept. The migration is time consuming and a new UC Booster Server needs to be set up. The migration ends in an OpenScape Business X V3 System with V2 mainboard and connected UC Booster Server V3.

A migration according to Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V3 with V3 Mainboard on page 1345 should be considered alternatively if customer data in the HX server need not to be kept.

Step 1 Migration of a HiPath 3000 System with OpenScape Office V3 HX to OpenScape Business V2

Within this step HiPath 3000 is migrated to OpenScape Business V2 and the UC functionality of the OpenScape Office V3 HX is mapped to an OpenScape Business UC Booster Server V2.

The UC Booster Server needs to be installed from scratch on a new HW and SW base. The licenses and customer data can be transferred from OpenScape Office V3 HX to the UC Booster Server if the UC Booster Server is set up first with OpenScape Business SW Version 1R2.2 only in this case the following UC configuration and user data are transferred:

- Announcements
- Images
- Voicemail
- Faxes
- Journal
- Contact Center Data
- User settings
- User Profiles
- External directory
- Schedules

The following UC configuration data and user data are **not** transferred and must be reconfigured in the UC Booster Server:

- Web services (e.g., XMPP, Web Collaboration, Mobility)
- Open Directory Service

After transferring licenses and customer data the UC Booster Server SW needs to be upgraded to SW version V1R3.3 and afterwards upgraded again to latest SW version V2R7.

For migration / upgrade perform the following steps in sequence:

1) **Record agent IDs** (only when using the Contact Center)

   Record the mappings of agent IDs to the stations of the UC Suite, since these assignments will not be migrated. The assignments must be reconfigured with the **UCD** wizard in the WBM of the OpenScape Business communication system.

2) **Update OpenScape Office V3 HX**

   First update the OpenScape Office V3 HX to the V3 R3FR6 software if this has not already been performed.

3) **Create an OpenScape Office V3 HX backup set**

   Create a backup set on an external device via the WBM of OpenScape Office V3 HX.

   More detailed information can be found in the online help of the OpenScape Office Assistant.

4) **Upgrade the HiPath 3000**

   Perform the upgrade from HiPath 3000 to OpenScape Business V1 as described in the migration procedure for a standalone system (see Migration of HiPath 33xx, 35xx, 3800 to OpenScape Business X3/X5/X8 V3 on page 1333). The licenses of the OpenScape Office V3 HX are transferred to OpenScape Business during the license migration at the license server. The license file contains the license data for both OpenScape Business X3/X5/X8 and the UC Suite.

5) **Setup UC Booster Server and integrate it in the customer LAN**

   The Linux operating system SLES 64 bit must be installed on the new server PC (Linux server), followed by the communication software (Version V1 R2.2). For details, please refer to the *OpenScape Business Linux Server Installation Guide*.

6) **Activate the UC Booster**

   Activate the UC Booster functionality in the WBM of the OpenScape Business communication system (**Basic Installation** > **Initial Installation** > **Package with UC Suite on OpenScape Business UC Booster Server**) and enter the IP address of the new server PC (using the same IP address as the old server PC if possible). Make sure that the UC Suite is active on the UC Booster Server.

   For more detailed information, see the section "Initial Installation of OpenScape Business X3/X5/X8" under How to Define the UC Solution on page 148.

7) **Configure the UC Booster**

   The IP address of the communication system must be specified in the WBM of the UC Booster Server.

   For more detailed information, see the section "Initial Installation of the OpenScape Business UC Booster" under Announcing the IP Address of the Communication System on page 274.

8) **Convert the OpenScape Office V3 HX backup set**

   The OpenScape Office V3 HX backup set saved on the external media must be converted via a Linux script to an OpenScape Business V1 backup set. To do this, you must be familiar with Linux. The converted backup set

must then be loaded into the UC Booster Server via the WBM. The UC configuration data and user data mentioned above will then be available.

More information on how to do this can be found in this section under How to Convert an OpenScape Office V3 HX Backup Set on page 1349.

9) **Update UC Booster Server software to V2**

First update the UC Booster Server to the Version V1 R3.3 and then to the latest OpenScape Business V2 software.

26.7.3.1 How to Convert an OpenScape Office V3 HX Backup Set

Prerequisites

The OpenScape Business UC Booster server is operational.

The OpenScape Office V3 HX backup set is available on the external medium.

Step by Step

1) Copy the OpenScape Office V3 HX backup set from the external medium to the server PC (Linux server) into the following directory:

   `/mnt/persistent/apollo/`

2) Open a terminal on the server PC or connect to it with an SSH shell. You will need root privileges for this.
3) Navigate to the backup directory with the following command:

   `cd /mnt/persistent/backup/`

4) Invoke the conversion script as follows:

   `/opt/symappl/services/backup/script/migrate.sh /mnt/persistent/apollo/<name of the backup set>`

   `/opt/symappl/services/backup/script/migrate.sh /mnt/persistent/apollo/BackupSet_130913-0400007.tar`

5) After the conversion script is run, the converted backup set can be used for the restore.

26.7.4 Migration of a HiPath 3000 network to OpenScape Business network

In order to upgrade a HiPath 3000 network to an OpenScape Business network, the following migration steps must be completed as described below.

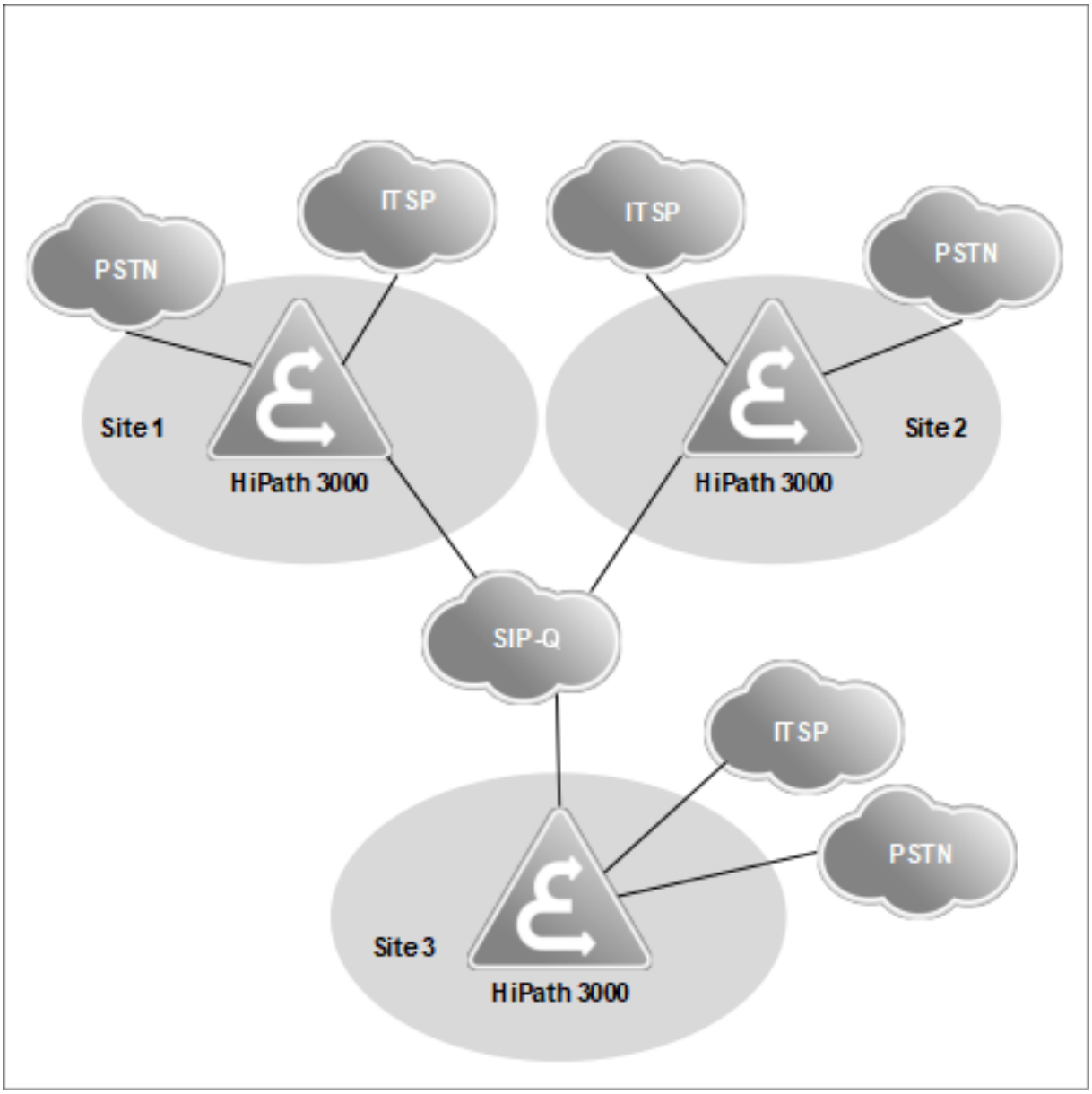


Figure 18: HiPath 3000 V9 Internetwork

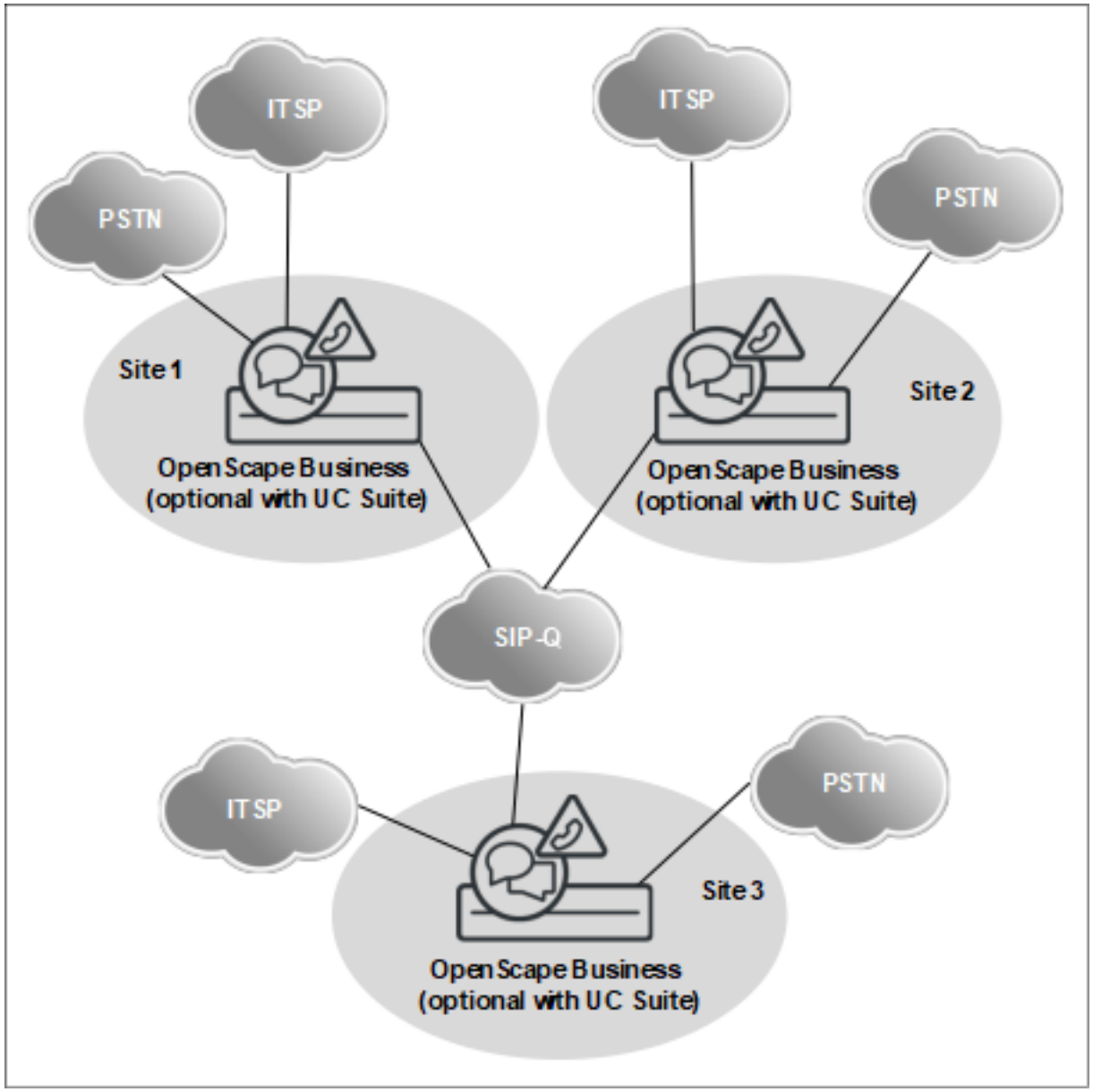


Figure 19: OpenScape Business Internetwork

Migration Steps

Perform the following steps in sequence:

1) **Upgrade the HiPath 3000**

   All HiPath 3000 systems of the internetwork must be upgraded separately according to the migration description for a standalone system (see 1.7.1).

2) **Edit the configuration**

   The following configuration parameters must subsequently be adapted using the WBM expert mode:

   - LCR entries
   - Voicemail system (hunt group, code to dial the voicemail)
   - Announcements

3) **Execute the licensing procedure.**

   Once all systems have been upgraded, the individual license files are combined into a network-wide license at the CLS.

26.7.5 Migration of a HiPath 3000 Internetwork with HiPath 5000 RSM

An HiPath 3000/5000 network with a common network license file can be broken down into standalone systems with individual license files via the Central License Server (CLS). Each standalone system is now migrated to OpenScape Business and licensed separately.

If required, the OpenScape Business systems can be merged to a network group with a single network license file at the CLS after migration.

The functionality of HiPath 5000 RSM has been integrated in OpenScape Business, hence HiPath 5000 RSM itself is no longer needed in the OpenScape Business internetwork.

For networking the OpenScape Business systems OpenScape Business Networking licenses must be available additionally per node.

For Internet telephony and T1 trunks additional trunk licenses are required.

The following migration steps must be completed as described bellow.

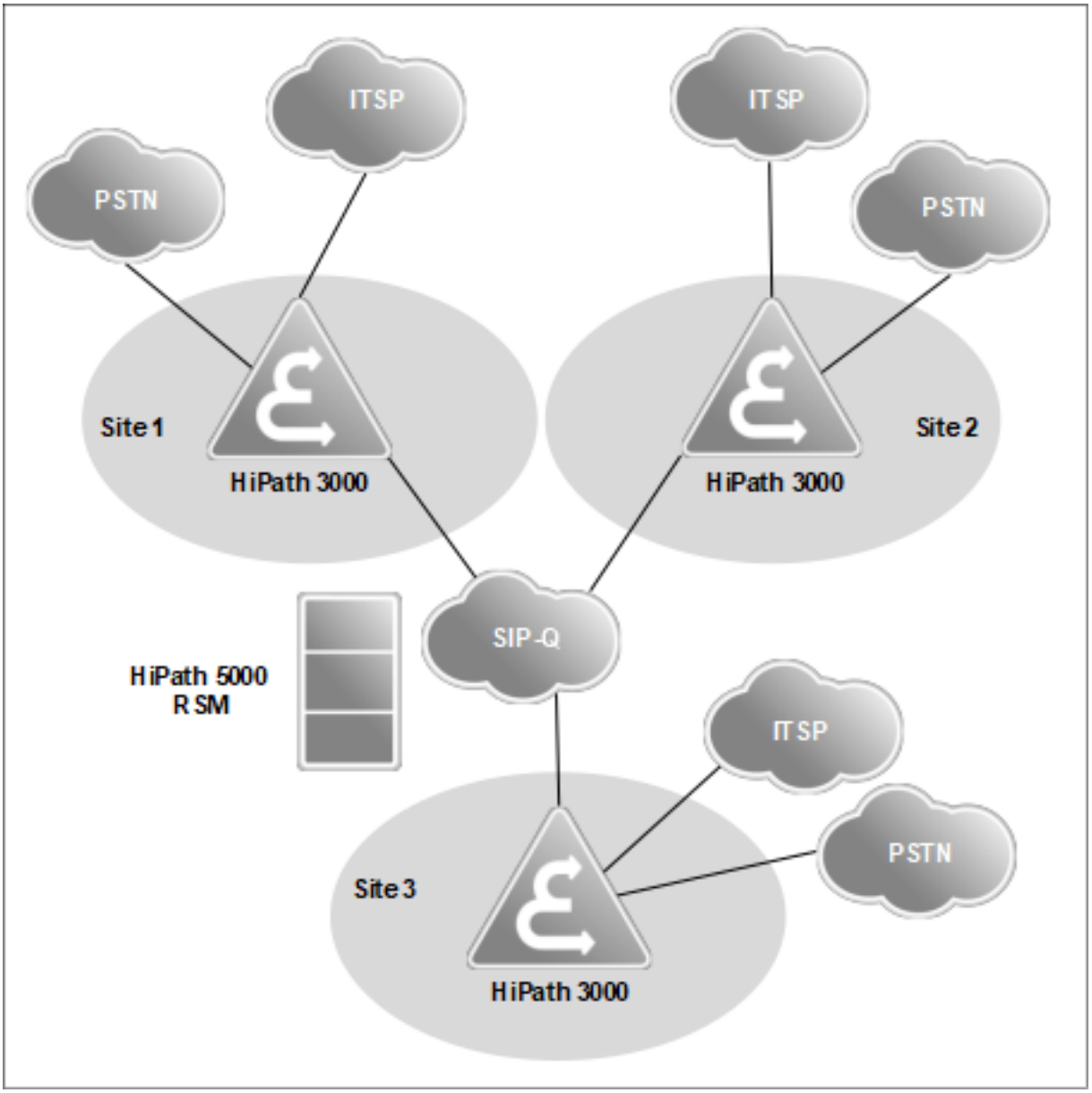


Figure 20: HiPath 3000 V9 Internetwork

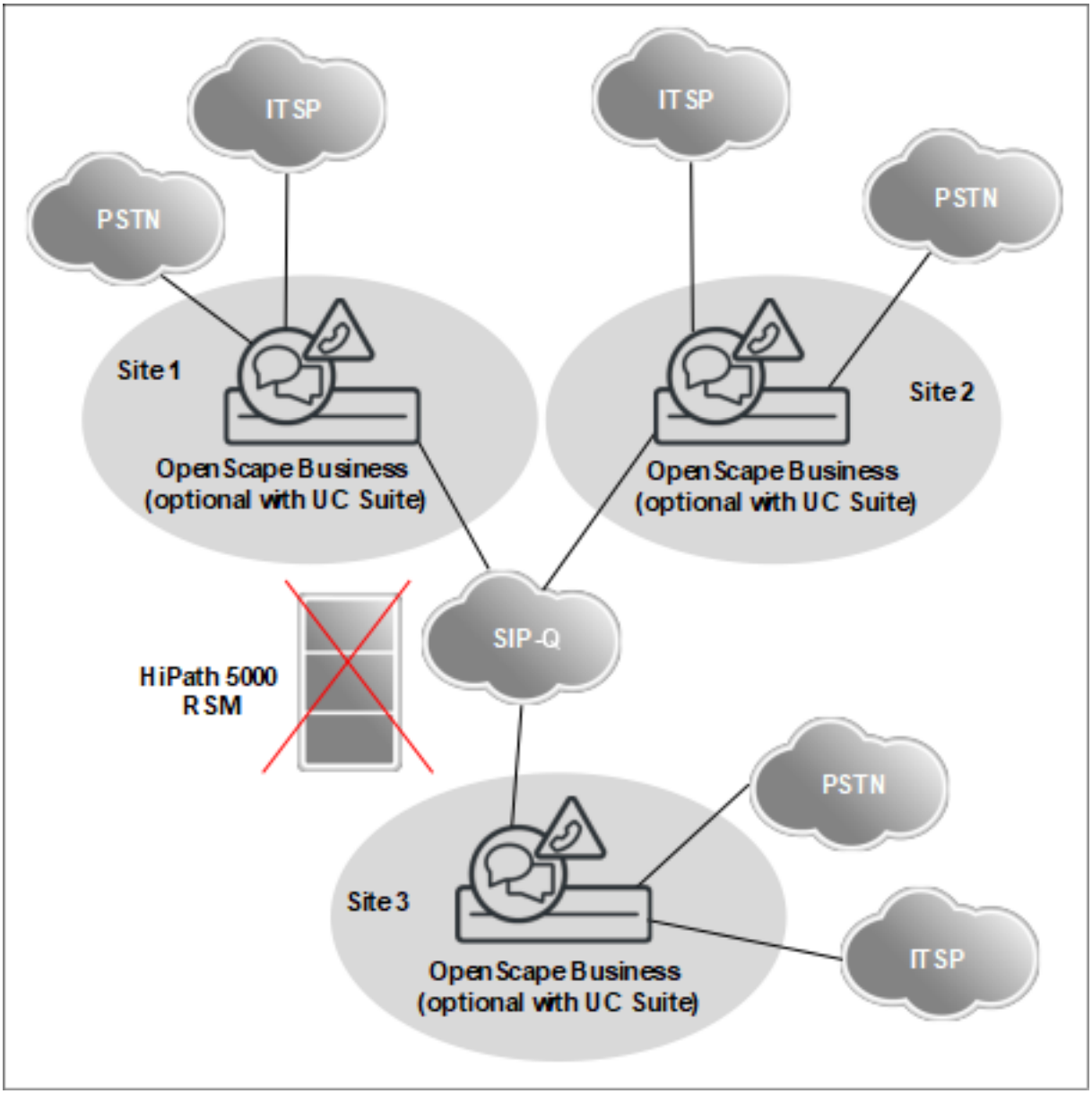


Figure 21: OpenScape Business Internetwork

Migration Steps

Perform the following steps in sequence:

1) Split the network license file into individual license files

A HiPath 3000 internetwork with HiPath 5000 RSM uses network-wide licensing. Split the network license file into individual license files at the CLS and assign those files to the locking IDs (MAC addresses) of the HiPath 3000 V9 systems before starting the actual migration to OpenScape Business.

- First, assign the licenses of the HiPath 5000 RSM internetwork to the individual locking IDs of the HiPath 3000 nodes. Recommendation: Create an Excel list in which the individual licenses are mapped to the locking IDs of the HiPath 3000 systems.

- Contact the licensing hotline and request that the licenses be split in accordance with the Excel list.
- Download the individual licenses of the HiPath 3000 systems from the CLS and check them. There is no need to activate the licenses, i.e., to transfer them to the HiPath 3000 systems.

2) **Remove HiPath 5000 RSM**

   Make sure that HiPath 5000 RSM is switched off before upgrading the HiPath 3000 systems.

3) **Upgrade the HiPath 3000**

   All HiPath 3000 systems of the internetwork must be upgraded separately according to the migration description for a standalone system. See 1.7.1

4) **Edit the configuration**

   The following configuration parameters must subsequently be adapted within OpenScape Business systems using the WBM expert mode:

   - LCR entries
   - Voicemail system (hunt group, code to dial the voicemail)
   - Announcements

5) **Execute the licensing procedure.**

   Once all systems have been upgraded, the individual license files of OpenScape Business are combined into a network-wide license at the CLS.

NOTICE: In case of a network-wide extension on UC functionality, it is necessary to change from open to closed numbering in order to adapt the internal numbers. Thus, the open numbering must be disabled, while the node number must be deleted and subsequently added as a prefix (for example, extended internal number 87100 instead of 100 and 88100 instead of 100).

Differences:

- The selection of participants in their own node is made with the extended internal number.

- The internal number and the DID number may differ if necessary, but the DID numbers must not be changed.

26.7.6 HiPath 3000 Changed/Dropped Features and Interfaces

Some HiPath 3000 features and interfaces have been adapted for OpenScape Business and enhanced in functionality.

Replacing the MMC Card

For technical reasons, the SDHC / M.2 SATA SSD card cannot be replaced while the system is switched on (a procedure which is known as speed update for HiPath 3000). Furthermore, the SDHC / M.2 SATA SSD card of a licensed system A cannot be used for another system B because the license is bound to the locking ID of mainboard A. If the SDHC / M.2 SATA SSD card is to be used in System B, it must be first initialized with new software by using the Card Manager.

HG1500 DSP channels / B channels

The HG1500 module is no longer required. The DSP functionality is integrated in OpenScape Business on the V3 motherboard and via optional Voice Channel Booster cards.

Please determine the number of DSP channels required. DSP channels are required to implement network transitions from TDM telephony to VoIP. OpenScape Business has 8 DSP channels integrated on the V3 mainboard. To extend DSP channels, the DSP module OCCB1/OCCBL (up to 40 channels) or the DSP module OCCB3/OCCBH (up to 120 channels) can be used.

entry Web Services

The entry Web Services are no longer supported. The successor to myPortal entry is called myPortal @work and provides extended functionality. myPortal for Mobile has been replaced by myPortal to go (Web Edition). The Plug PC is no longer required in order to use myPortal to go

Entry Voicemail

The Entry Voicemail module is dropped in OpenScape Business - the function is integrated as Smart Voicemail in the OpenScape Business mainboard. Smart Voicemail users must be licensed.

External Voicemail

If the HiPath 3000 uses an external voicemail solution such as Xpressions, the ten EVM ports must be changed from **PhoneMail** to **Standard** in Manager E after CDB conversion.

Enhanced SIP Functionality

The following SIP features have been additionally implemented as compared to HiPath 3000 V9:

- Call completed elsewhere
- Message Waiting Indication for Voicemail
- Calling Name Presentation (CNIP)
- Distinctive Ringing (internal/external calls)
- 3rd Party Call Control
- Call Forwarding busy/no reply/unconditional (handset controlled)

SIP Trunking

To connect external SIP servers (e.g., OpenScape Alarm Server, HiPath 4000, OpenScape Voice or UC Suite), additional native SIP/SIP-Q routes are available in OpenScape Business (as opposed to only one SIP-Q route in HiPath 3000). Thus, in addition to the classical routes for the CO, networking and ITSP, independent native SIP/SIP-Q trunk interfaces (called the SIP Interconnection) are provided for certified SIP applications.

See Networking OpenScape Business

LCR

Routing tables 1 to 15 are intended for default entries or for configuration using wizards. During a migration, the existing entries in the HiPath 3000 are not transferred to these routing tables. Manual post-processing of the routing tables is therefore required.

Simplified Dialing

Either the "LCR" function or the "Prime Line (Simplified dialing)" function can be activated but not both at the same time. For this reason, "LCR" is activated automatically during migration while "Prime Line (Simplified dialing)" is deactivated. To deactivate "LCR" and to activate "Prime Line (Simplified dialing)", the Basic Installation wizard must be completed before the relevant flags can be set in Manager E (not for OpenScape Business X1 because it does not allow administration via the Manager E).

NOTICE: Simplified dialing is not supported in CSTA applications.

VoIP over PPP via ISDN

Routed voice calls over lines with low bandwidth are no longer supported.

G.723 support

G.723 codecs are no longer supported.

Babyphone

The Babyphone (room monitoring) feature is no longer supported. Since "CSTA monitoring" is always active (a system phone can be monitored by an application such as myAgent or myPortal, for example), "room monitoring" can no longer be activated for this system phone. During CDB conversion with Manager E, the code for activating the room monitor is deleted.

Number of Base Stations and DECT Telephones at OpenScape Business X3

The number of base stations at OpenScape Business X3 was increased from 3 to 7 as compared to HiPath 33xx. The number of DECT telephones at OpenScape Business X3 was increased from 16 to 32 as compared to HiPath 33xx.

HiPath 3000 BS4

Base station licenses are no longer required in OpenScape Business.

SSDP based on the Plug PC

SSDP is integrated in OpenScape Business. The Plug PC is no longer required.

Accounting interface

The interfaces of the accounting data have changed compared to HiPath 3000.

V24 applications

V24 applications are no longer supported.

CSTA applications

Within OpenScape Business V3 either a V3 mainboard or a UC Booster Card / Server in combination with a V2 mainboard is required for connecting CSTA applications. In an internetwork, a V3 mainboard / UC Booster Card / Server must exist only in the master node. The applications must support the CSTAv3 protocol. Compared with HiPath 3000, changes have been implemented to the

CSTA protocol. Consequently, CSTA applications at HiPath 3000 V9 may not run compatibly at OpenScape Business systems. The CSTAv2 protocol is no longer supported.

In SW Version 3 a CSTA license is required for used of the CSTA interface with following except for:

- UC Booster Card CSTA connections in general
- OpenScape Business TAPI 120 or TAPI 170 CSTA connections in general

Compared to the HiPath 3000 CSTA interface, the OpenScape Business CSTA interface has been modified as follows:

- The connection to the CSTA interface is identical for standalone and networked OpenScape Business slave node. CSTA at master node in a network provides enhanced functionality. It occurs exclusively via the LAN. RS-232 (V.24) and S0 interfaces are no longer supported.
- Additional hardware and software components such as the CSTA Service Provider (CSP), HG 1500 board or HiPath 5000 RSM System are no longer required with OpenScape Business. Instead UC Booster HW or V3 mainboards are required.
- The CSTA interface is licensed with exception of UC Booster Card and TAPI 120/170 connections.
- A maximum of 4 CSTA links can be used for connecting external applications. In the default factory state, 3 of the 4 CSTA interfaces are preconfigured for the use of internal applications of OpenScape Business. These can optionally also be used for connecting external applications.
- The protection of the CSTA interfaces against abuse has been improved. The access mechanism has been revised.
- MULAP monitoring via CSTA is only possible if a monitor point is set on the MULAP number. Individual MUALP members cannot be monitored. If a CSTA application would nonetheless like to monitor individual MULAP members, no CSTA events will be transmitted to the application by OpenScape Business. This also applies to MULAP members who are part of a hunt group.
- The provided CSTA functions have been expanded. Details can be found in the OpenScape Business CSTA Interface Manual.
- The CSTA Phase II protocol version is no longer supported.
- CSTA applications to be used with OpenScape Business should be tested and released in conjunction with OpenScape Business.

HiPath TAPI 120/170 V2 Applications

For HiPath TAPI 120/170 V2, the existing licenses cannot be transferred. New licenses must be purchased. HiPath TAPI 120/170 V2 must be uninstalled, and OpenScape Business TAPI 120/170 V1 must be installed and configured instead.

TAPI licenses can be configured in OpenScape Business on a user basis, thus elimination the need for TAPI licensing within the TAPI device. Licensing is required as of the first TAPI user (so even TAPI120 is thus no longer license-free for the first 6 users). The CMD (CSTA Message Dispatcher) is integrated in OpenScape Business. A separate Windows server for the CMD is therefore no longer required. Connectivity to external TAPI applications is possible for OpenScape Business and OpenScape Business S. OpenScape Business requires a V3 Mainboard or a UC Booster Card / Server. In an internetwork, either an OpenScape Business S must exist, or a V3 mainboard / UC Booster Card / Server must exist at least on the master node.

Compared to HiPath TAPI 120/170 V2, the OpenScape Business TAPI 120/170 V2 V1 has been modified as follows:

- Access to the system is only possible via Ethernet LAN. RS-232 und S0 interfaces are no longer supported.
- New shared TAPI license on a "per user" basis for TAPI 120 TSP und TAPI 170 TSP.
- The licenses are bound to the locking ID of OpenScape Business.
- Existing HiPath TAPI 120 TSP or HiPath TAPI 170 TSP user licenses are not supported by the new licensing mechanism.
- No backward compatibility with HiPath 3000 V8 or V9
- The following applies for TAPI 170 TSP:
  - By default, access to the system occurs via Port 8800.
  - The configuration of the CSTA credentials in the setup dialog is mandatory.
  - Multi-node support in the network via the CSP of the central master node.
- The following applies for TAPI 120 TSP:
  - By default, access to the system occurs via Port 8900.
  - Single-node support, even when connected to the master node of a network.

Other External Applications

Subsequent applications connected externally to HiPath 3000 can no longer be operated on OpenScape Business.

HiPath 3000 Application	Successor Application for OpenScape Business	Remarks
optiClient Attendant	OpenScape Business Attendant	New application No license transfer possible
optiClient BLF V1/V2	OpenScape Business Attendant (OpenScape Business BLF)	New application No license transfer possible
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	New application No license transfer possible
Communication Clients der Entry WEB Services on Plug PC	Integrated UC Solution	New application No license transfer possible
myPortal for Mobile/ Tablet	myPortal to go	New application No license transfer possible

HiPath 5000 RSM Changed/Dropped Features

HiPath 5000 RSM is no longer supported. The functionality of HiPath 5000 RSM has been integrated into OpenScape Business. This means that a separate server is no longer required.

Table 37: Differences between HiPath 5000 RSM and OpenScape Business V3

Feature	HiPath 5000 RSM	OpenScape Business
Network-wide licensing, assignment of licenses to the individual nodes	All system licenses of the network are combined at the CLS into a network-wide license.	All system licenses of the network are combined at the CLS into a network-wide license.
Network-wide administration	DB Feature Server: all nodes of the network are combined into a network CDB using Manager E. The numbering scheme is synchronized across the network.	All nodes of the network are recorded through the OpenScape Business Assistant (WBM) with a network wizard. The numbering scheme is synchronized network-wide (closed numbering).
Connection to external nodes or external applications	SIP-Q connection of up to 4 external nodes	Up to 10 SIP interconnection routes with up to 2 SIP-Q or up to 10 Native SIP or up to 8 ITSP
Resilience / Survivability	User survivability for HFA phones with closed numbering	User survivability for HFA phones with closed numbering (change from OpenScape Business S <-> OpenScape Business X3/X5/X8)
Backup / Restore	Netwide	Local
Inventory function	Netwide	Local
Presence Manager	Network-wide function with the provision of 5000 RSM	Network-wide function with the provision of a multi-node CSP based on the OpenScape Business UC Booster Card, the OpenScape Business UC Booster Server or OpenScape Business S. Prerequisite: closed numbering.

Feature	HiPath 5000 RSM	OpenScape Business
TAPI 170 on a standalone system	TAPI 170 on a standalone system runs on a Windows PC with its own licensing (separate license file for the TAPI 170).	TAPI 170 on a standalone system runs on a Windows PC. The license request and supply of the TAPI 170 database occurs from the SQL DB of OpenScape Business. The connection of the TAPI 170 occurs via the CSP of the system (OpenScape Business UC Booster Card, OpenScape Business UC Server Booster or OpenScape Business S)
TAPI 170 in an Internetwork	TAPI 170 runs on 5000 RSM with its own licensing (separate license file for the TAPI 170). The TAPI 170 database is obtained from the DB Feature Server of the 5000 RSM.	As with the standalone system, but the connection of the TAPI 170 occurs at the multinode CSP of a master node (i.e., network-wide). Prerequisite: closed numbering.

Mixed Networks

Mixed internetworks consisting of OpenScape Business and OpenScape Office are not supported.

26.8 Migration within OpenScape V3 Business

The various migration options within OpenScape Business X V3 systems with V2 mainboards are described here.

NOTICE: These scenarios are obsolete (not valid) for OpenScape Business X V3 systems with V3 mainboards!

Increasing the Number of UC Smart Users

You can choose from the following options:

- Migration of **OpenScape Business X** (UC Smart) to **OpenScape Business X** with **UC Booster Card** (UC Smart)

  Useful for 50 to 150 UC Smart users. All the configuration and user data is transferred. No data transfer occurs with downgrades. Additional UC user licenses are required for the new UC Smart users. OpenScape Business X1 is not expandable with the UC Booster Card.

- Migration of **OpenScape Business X** (UC Smart) to **OpenScape Business X** with **UC Booster Server** (UC Smart)

  Useful for 50 to 500 UC Smart users. All the configuration and user data is transferred. No data transfer occurs with downgrades. Additional UC user licenses are required for the new UC Smart users.
- Migration of **OpenScape Business X** with **UC Booster Card** (UC Smart) to **OpenScape Business X** with **UC Booster Server** (UC Smart)

  Useful for 150 to 500 UC Smart users. All the configuration and user data is transferred. No data transfer occurs with downgrades. Additional UC user licenses are required for the new UC Smart users.

Upgrade from UC Smart to UC Suite

You can choose from the following options:

- Migration of **OpenScape Business X** (UC Smart) to **OpenScape Business X** with **UC Booster Card** (UC Suite)

  The configuration and user data is not transferred. An upgrade license to UC Suite clients is required for the existing UC Smart clients. The conversion of the UC solution to UC Suite occurs in the WBM with the **Initial Installation** wizard.
- Migration of **OpenScape Business X** (UC Smart) to **OpenScape Business X** with **UC Booster Server** (UC Suite)

  The configuration and user data is not transferred. An upgrade license to UC Suite clients is required for the existing UC Smart clients. The conversion of the UC solution to UC Suite occurs in the WBM with the **Initial Installation** wizard.
- Migration of **OpenScape Business X** with **UC Booster Card** (UC Smart) to **OpenScape Business X** with **UC Booster Server** (UC Suite)

  The configuration and user data is not transferred. An upgrade license to UC Suite clients is required for the existing UC Smart clients. The conversion of the UC solution to UC Suite occurs in the WBM with the **Initial Installation** wizard.
- Migration within **OpenScape Business S** from UC Smart to UC Suite

  The configuration and user data is not transferred. An upgrade license to UC Suite clients is required for the existing UC Smart clients. The conversion of the UC solution to UC Suite occurs in the WBM with the **Initial Installation** wizard.
- Migration within **OpenScape Business UC Booster Server** from UC Smart to UC Suite

  The configuration and user data is not transferred. An upgrade license to UC Suite clients is required for the existing UC Smart clients. The conversion of the UC solution to UC Suite occurs in the WBM with the **Initial Installation** wizard.

Increasing the Number of UC Suite Users

You can choose from the following options:

- Migration of **OpenScape Business X** with **UC Booster Card** (UC Suite) to **OpenScape Business X** with **UC Booster Server** (UC Suite)

  Useful for 150 to 500 UC Suite users. All the configuration and user data is transferred. No data transfer occurs with downgrades. Additional UC User or Groupware User licenses are required for the new UC Suite users.

26.9 Migration of HW boards

The following hardware migration actions are possible in case of an OpenScape Business X8 system:

- Replacements of SLMO24N with SLMU
- Replacements of SLMO8N with SLMU
- Replacements of SLCN with SLMUC (SLMU + CMAe)

26.9.1 Replacement of SLMO24N with SLMU

A simple card exchange is supported. The SLMO24N can be removed from the system and the new SLMU can be plugged. All configured prots are kept unchanged. There is no need to switch off the system.

26.9.2 Replacement of SLM8N with SLMU

As the SLMU card has more ports than the SLMO8, the SLMO8 card must be removed per administration. In order to remove the card from the system, the Online User with the following dialog should be used:

```
Systemadministration 29- 4 - 1
```

and change the card type to SLMUC.

NOTICE:

If the users are configured for UC Suite, they are created with the default settings. All previous data (for example, Voicemail, Fax, User settings) are lost.

NOTICE:

If the SLMO8 is exchanged with the SLMU card without removing the card with the described procedure, the additional 16 ports from the SLMU card might be lost as they could not be configured. This will happen if there is already another card in operation using the port range of these 16 ports. If there is a single SLMO8 in the system, replaced by an SLMU card, all ports will be available.

26.9.3 Replacement of SLCN with SLMUC (SLMU plus CMAe)

As the SLMU card has more ports than the SLCN, the SLCN must be removed per administration before the SLMUC go into service in that slot. The process to remove the card is the following:

1) **De-Register all CMI handsets from their Base Station**
2) **Remove the card from the system**
3) **Remove the SLCN card per Online User with the dialog:**

   `Systemadministration 29- 4 - 1`

   and change the card type to SLMUC.
4) **Install the SLMUC card**
5) **Configure the used Handset**
6) **Register the CMI handsets**

   All affected DECT Phones (maximum of 128) have to be connected for the new registration.

NOTICE:

When replacing an SLCN card by an SLMUC, it is also needed a blind cover for the SLMUC instead of the plastic cover which is used for the SLCN.

NOTICE:

If the users are configured for UC Suite, they are created with the default settings. All previous data (for example, Voicemail, Fax, User settings) are lost.

26.10 Migration from OpenScape Business X1 V2 to OpenScape Business X1W V3

When migrating an OpenScape Business X1 model, the complete system needs to be replaced.

Existing licences can be taken over. The customer configuration cannot be taken over and must be restored manually after the migration. The existing software support will be continued unchanged after the migration or a new software support date for the V3 mainboard will be adopted if this is valid beyond 31/12/2026.

Before the migration, permanent access to the Unify license server (via the Internet) should be set up in the system, if not already available, and the "CLS Connect" function should be activated. This simplifies the license transfer and shortens the migration time considerably. The customer must be informed about the required access from the OpenScape Business System to the CLS.

Required order items

For the migration of the X1 model to X1W with V3 mainboard, the following order items are required depending on whether CLS Connect, UC Suite or external CSTA applications are used:

- X1W System
- V3 SW on M.2 SATA SSD data storage
- M2 SSD 256 GB mass data storage (optional with UC Suite application)
- OpenScape Business Upgrade for OS Biz X1 license (is always needed)
- OpenScape Business CSTA license (optional)

Functional boundary conditions

Existing licenses can be transferred completely from the existing X1 System to the X1W System with V3 mainboard in the course of the migration. License transfer without activating the CLS Connect function requires the "Migration" license and a much more complex handling and a higher time expenditure than using the CLS Connect function.

X1 systems with active CLS Connect cannot be upgraded to X1W systems with V3 mainboard via the "Regeneration" function. The license "OpenScape Business Upgrade for OS Biz X1" must always be activated, but no confirmation code must be entered during the upgrade process.

Upgrading OpenScape Business X1 PAYGO system to OpenScape Business X1W PAYGO systems is not supported.

In the event that OpenScape Personal Edition clients are operated on the system and corresponding licenses are available, these must always be regenerated manually at the central license server for the new locking ID (MAC address) of the V3 mainboard, regardless of whether CLS Connect is used or not.

The customer configuration cannot be taken over and must be restored manually after the migration.

Technical handling of the migration

The main technical steps of the migration are described below. A distinction is made between:

- Migration with permanent licensing
  - Migration with activated CLS Connect function and connection to the central license server
  - Migration without CLS Connect function and without connection to the central license server

Further details about the technical handling of the migration are contained in the OpenScape Business Administrations manual.

26.10.1 How to Migrate to X1W V3 Permanently Licensed Systems with CLS Connect

Step by Step

1) Generate license files at the Central License Server (CLS).

a) Activate the “OpenScape Business Upgrade for OS Biz X1” license on the X1 system with V2 mainboard. During the activation process provide the V3 mainboard MAC address.

b) Generate a new license file for the MAC address of the X1W system with V3 mainboard. This license file includes the extended SW support.

c) Transfer of possibly existing Personal Edition licenses from the MAC address of the V2 mainboard to the MAC address of the V3 mainboard using the "Regenerate" function and generation of a new license file for the Personal Edition licenses.

2) Prepare the OpenScape Business System.

a) Upgrade the existing system to SW version V2R7.

b) Set up access to the Central License Server (CLS) in the system and test the connection.

c) Activate CLS Connect in the system. If not already done, SW support will be extended again for 3 months.

3) X1 System exchange

a) X1 System shut down and switch off all supply voltages.

b) Use V3 data carrier and if necessary optional mass data storage on the X1W System.

c) Remove the CAMe and or the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the X1W V3 mainboard.

d) Replace the X1 System by the X1W system.

e) Connect the grounding cable to the X1W system.

f) Connect the telephone, trunk line, LAN and, if applicable, USB cables to the X1 W system.

g) Switch on supply voltages again, system boots automatically.

4) Set Basic System Parameters within WBM after startup.

a) Set system date and time.

b) Set application package.

- UC Smart for systems without UC or with UC Smart
- UC Suite for systems with UC Suite

c) Restore the system configuration.

- Manual configuration of the X1W.
- Importing the newly created license files.

26.10.2 How to Migrate to X1W V3 Permanently Licensed Systems without CLS Connect

Step by Step

1) Prepare OpenScape Business System.

a) Upgrade the existing system to SW version V2R7.

2) Create a migration license file for the X1 with V2 mainboard at the central license server (CLS).

a) Activation of the "X1 Migration License" for the existing system.

b) Generate the new license file for the MAC address of the V2 mainboard. For this, the MAC address of the X1W system must be entered at the CLS.

c) Downloading the license file from CLS. This license file includes the extended SW support.

3) Import the license file into the OpenScape Business X1 System with V2 mainboard.

4) Note the "Confirmation Code" displayed in OpenScape Business Assistant.

5) Generate a new license file for the X1W system with V3 mainboard at the central license server (CLS).

a) Create a new license file for the MAC address of the X1W System with V3 mainboard at the CLS by regenerating the MAC address of the X1 with V2 mainboard and the previously noted confirmation code.

- Search for the OpenScape Business System with the MAC address of the X1W System with V3 mainboard in the CLS.
- Unlocking the OpenScape Business System by entering and activating the Confirmation Code.
- Regenerate the license file.

b) Download the newly generated license file from CLS.

6) Mainboard exchange

a) Shut down the system and switch off all supply voltages.

b) Use V3 data carrier and if necessary optional mass data storage on the X1W System with the V3 mainboard.

c) Remove the CAMe and or the OCCB Voice Channel Booster card from the V2 mainboard and plug it into the X1W with V3 mainboard.

d) Replace the X1 System withV2 mainboard with the X1W System with V3 mainboard.

e) Connect the grounding cable to the X1W system.

f) Connect the telephone, trunk line, LAN and, if applicable, USB cables to the X1 W system.

g) Switch on the power supply again and the system boots automatically.

7) Set Basic System Parameters within WBM after startup.

a) Set system date and time.

b) Set application package.

- UC Smart for systems without UC or with UC Smart
- UC Suite for systems with UC Suite

c) Restore the system configuration.

- Manual configuration of the X1W

d) Manual import of the new license file into the V3 system after system startup.

27 Configuration Limits and Capacities

The configuration limits and capacities are based on system-specific maximum values of a single system. The maximum values of a system in a network can be different.

27.1 Maximum values for stations

- Data for systems with V2 OCC mainboards can be found in Table 38: Expansion Level Stations/Users with OCCx mainboards on page 1368
- Data for systems with V3 OCC mainboards can be found in Table 39: Expansion Level Stations/Users with OCCSB/R, OCCMA/B or OCCLA mainboards on page 1369
- Data for OpenScape Business S Server systems can be found in Table 40: Expansion Level Stations/Users with OpenScape Business S on page 1370

Table 38: Expansion Level Stations/Users with OCCx mainboards

Stations	X1	X3W/R	X5W/R	X8
Stations maxium				
Max. number of stations[16]	30	500	500	500
IP stations				
IP-Stations System (HFA)	20[17]	500	500	500
IP-Stations (SIP)	20[17]	500	500	500
TDM stations				
Max. number of TDM Stations[18] [22]	30	384	384	384
Analog stations (TDM)	4	20	68	384
U_{P0} Master stations (TDM)[22]	8	24	56	384
U_{P0} Slave stations (TDM) (incl. a/b and S0 adapters)	8	24	56	116
S0 ISDN stations (TDM)	2	36	52	128
DECT-CMI stations (TDM)	16	64	64	250
Mobility User				
Max. number of mobility users[19]	30	150	150	150
Mobility Entry users	20	150	150	150
myPortal to go users[20]	30	150	150	150
Skype for Business users	30	150	150	150
Other users				
RAS users	2	500	500	500

Stations	X1	X3W/R	X5W/R	X8
Virtual stations freely configurable	30	250	250	250

NOTICE: For each system configuration, it must be checked whether the rated power output of the native power supply is sufficient or whether an external auxiliary power supply is required (see *OpenScape Business Service Documentation - Power Requirements of a Communication System*).

Table 39: Expansion Level Stations/Users with OCCSB/R, OCCMA/B or OCCLA mainboards

Stations	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Stations maximum								
Max. number of stations[16]	500	500	500	500	500	500	500	500
IP stations								
IP-Stations System (HFA)	500	500	500	500	500	500	500	500
IP-Stations (SIP)	500	500	500	500	500	500	500	500
TDM stations								
Max. number of TDM Stations[18 22]	30	30	384	384	384	384	384	384
Analog stations (TDM)	4	4	20	20	68	68	384	384
U_{P0} Master/Slave stations (TDM)[22]	8	8	24	24	56	56	384 master 116 slave	384 master 116 slave

15 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

16 Sum of: IP (HFA), IP (SIP), Analog, UP0 Master/Slave, DECT (CMI), ISDN S0, Mobility and Deskshare subscribers

17 Sum of IP user and desk share user (limitation via configuration)

18 Sum of: Analog, UP0, DECT (CMI) and ISDN S0 subscribers

19 Sum of: Mobility Entry, myPortal to go- Skype for Business participants

20 The number of simultaneous VoIP connections of the subscriber depends on:

1) the DSP channels available in the system for gateway calls (IP/TDM transition).

2) the internal RTP proxy channels available in the system for VoIP calls via the Internet.

21 The number of simultaneous connections depending on the DSP channels available in the system for gateway calls (IP/TDM transition).

22 Depending on the types of phones and the total power requirements of the communication system

Stations	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
S0 ISDN stations (TDM)	0	0	32	32	48	48	128	128
DECT-CMI stations (TDM)	16	16	64	64	64	64	250	250
Mobility User								
Max. number of mobility users[19]	150/ 500[23]	150/ 500[23]	150/ 500[23]	150/ 500[23]	150/ 500 [23]	150/ 500[23]	500	500
Mobility Entry users	150	20	150	150	150	150	150	150
myPortal to go users[20]	150/ 500[23]	30	150/ 500[23]	150/ 500[23]	150/ 500[23]	150/ 500[23]	500	500
myPortal for Teams users[20]	150/ 500[23]	30	150/ 500[23]	150/ 500[23]	150/ 500[23]	150/ 500[23]	500	500
Skype for Business users	150/ 500[23]	30	150/ 500[23]	150/ 500[23]	150/ 500[23]	150/ 500[23]	500	500

Table 40: Expansion Level Stations/Users with OpenScape Business S

Stations	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Stations maxium			
Max. number of stations	50	500	1500
IP stations			
IP-Stations System (HFA)	50	500	1500
IP-Stations (SIP)	50	500	500
Mobility User			
Max. number of mobility users	50	250	500
Mobility Entry users	50	150	150
myPortal to go users	50	250	500
myPortal for Teams users	50	250	500
Skype for Business users	50	250	500

27.2 Maximum values for lines

- Channels of all kind of lines (trunk, tie, interconnection lines, etc.) in V2 OCC mainboards can be found in Table 41: Expansion Level Line Channels with OCCx mainboards on page 1371.

[23] Values are staggered according to Board version: Basic/Advanced

- Channels of all kind of lines (trunk, tie, interconnection lines, etc.) in V3 OCC mainboards can be found in Table 42: Expansion Level Line Channels with OCCSB/R, OCCMA/B or OCCLA mainboards on page 1371
- Channels of all kind of lines (trunk, tie, interconnection lines, etc.) in OpenScape Business S can be found in Table 43: Expansion Level Line Channels with OpenScape Business S on page 1372

Table 41: Expansion Level Line Channels with OCCx mainboards

	X1	X3W/R	X5W/R	X8
Line channels maximum				
Max. number of line channels[24]	250	250	250	250
Line channels for connection of telephony service provider, networking, external computer				
SIP trunk channels (ITSP)	30	60[25]	60[25]	60[25]
SIPQ-channels (Networking)	100	100	100	100
ISDN S_0 - channels (BRI)	4	20	52	128
ISDN S_{2M} - channels (PRI)	-	30	30	80
ISDN CAS - channels (PRI)	-	30	30	180
Analog (a/b) channels	-	X3R: 8 X3W: 16	X5R: 24 X5W: 48	120
Line channels for internal purposes				
MEB channels for internal announcements[26]	0	16	16	16
MEB Trunk channels for UC Suite[27]	0	60 / 30 / 0[28]	60 / 30 / 0[28]	60 / 30 / 0[28]

Table 42: Expansion Level Line Channels with OCCSB/R, OCCMA/B or OCCLA mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Line channels maximum								
Max. number of line channels[24]	250	250	250	250	250	250	250	250

24 Sum of; SIP trunk, ITSP, SIPQ, TDM line channels and MEB Trunk channels w/o (MEB announcement channels).

25 In networking with OpenScape Business S as ITSP gateway, more than 60 channels are also possible

26 The MEB channels are dynamically assigned by the system for system-internal announcements. They are always included in the maximum number of line channels.

27 For systems with UC Suite, the MEB channels are dynamically generated for: Voicemail, AutoAttendant, Fax, Call Me connections, announcements and conference calls. They only count towards the maximum number of line channels in UC Suite systems.

28 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Line channels for connection of telephony service provider, networking, external computer								
SIP trunk channels (ITSP)	60/ 120[29]	60/ 120[29]	60/ 120[29]	60/ 120[29]	60/ 120[29]	60/ 120[29]	120	120
SIPQ-channels (Networking)	100	100	100	100	100	100	100	100
ISDN S_0 - channels (BRI)	-	-	16	16	48	48	128	128
ISDN S_{2M} - channels (PRI)	-	-	30	30	30	30	180	120
ISDN CAS - channels (PRI)	-	-	30	30	30	30	180	120
Analog (a/b) channels	-	-	X3R: 8 X3W: 16	X3R: 8 X3W: 16	X5R: 24 X5W: 48	X5R: 24 X5W: 48	120	120
Line channels for internal purposes								
MEB channels for internal announcements[26]	16	16	16	16	16	16	16	16
MEB Trunk channels for UC Suite[27]	0	30/60[29]	0	30/60[29]	0	30/60[29]	0	60

Table 43: Expansion Level Line Channels with OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Line channels maximum			
Max. number of line channels[24]	250	250	250
Line channels for connection of telephony service provider, networking, external computer			
SIP trunk channels	180	180	180
SIPQ-channels (Networking)	100	100	100
Line channels for internal purposes			
MEB channels for internal announcements[26]	16	16	16
MEB Trunk channels for UC Suite[27]	60	60	60

[29] Values are staggered according to Board version: Basic/Advanced

27.3 Maximum values for resources

Table 44: Expansion Level other functions / resources

	X1		X3		X5		X8	Server (S)
	Rack	Wall	Rack	Wall	Rack	Wall	OCCL / OCCLA	
System resources								
DSP-channels								
DSP G.711 without encryption	8	8	128/ 48/ 8[35]	128/ 48/ 8[35]	128/ 48/ 8[35]	128/ 48/ 8[35]	128/ 48/ 8[35]	n/a
DSP G.711 + G.729 without encryption	8	8	104/ 40/ 8[35]	104/ 40/ 8[35]	104/ 40/ 8[35]	104/ 40/ 8[35]	104/ 40/ 8[35]	n/a
DSP G.711 with encryption	6	6	102/ 38/ 6[35]	102/ 38/ 6[35]	102/ 38/ 6[35]	102/ 38/ 6[35]	102/ 38/ 6[35]	n/a
DSP G.711 + G.729 with encryption	6	6	81/ 31/ 6[35]	81/ 31/ 6[35]	81/ 31/ 6[35]	81/ 31/ 6[35]	81/ 31/ 6[35]	n/a
DSP Fax T.38 (for ISDN Gateway)[33]	3	3	12/ 6/ 3[35]	12/ 6/ 3[35]	12/ 6/ 3[35]	12/ 6/ 3[35]	12/ 6/ 3[35]	n/a
DSP Fax T.38 (for UC Suite Fax)[34]	-	-	8/ 6/ 0[35]	8/ 6/ 0[35]	8/ 6/ 0[35]	8/ 6/ 0[35]	8/ 6/ 0[35]	n/a
RTP Proxy channels								
RTP Proxy channels	30	30	60	60	60	60	60	180
MEB-line channels								
MEB-line channels in total	**0**	**0**	**76/ 46/ 0[31]**	**76/ 46/ 0[31]**	**76/ 46/ 0[31]**	**76/ 46/ 0[31]**	**76/ 46/ 0[31]**	**76**
MEB-line channels for announcements	0	0	16/ 16/ 0[31]	16/ 16/ 0[31]	16/ 16/ 0[31]	16/ 16/ 0[31]	16/ 16/ 0[31]	16
MEB-line channels for UC Suite	-	-	60/ 30/ 0[31]	60/ 30/ 0[31]	60/ 30/ 0[31]	60/ 30/ 0[31]	60/ 30/ 0[31]	60
Music on hold and PPP								

	X1		X3		X5		X8	Server (S)
	Rack	Wall	Rack	Wall	Rack	Wall	OCCL / OCCLA	
MOH sources [30] (G.711a, G.711u, G.729ab, G.729a)	4	4	4	4	4	4	4	32
PPP channels	8	8	8	8	8	8	8	n/a
Announcements								
Number of announcement devices per system	16	16	16	16	16	16	16	16
Announcement devices via a/b	4	4	16	16	16	16	16	n/a
Announcements via Smart VM	6	6	6	6	6	6	6	6
Announcement via UC-Suite	16	16	16	16	16	16	16	16
Announcement before answering (system, not UC-Suite)								
Number of callers for whom an announcement can be played simultaneously	24	24	24	24	24	24	24	24
DTMF receiver								
DTMF receiver	16	16	16	16	16	16	16	Per call via ITSP

27.3.1 Details on the use of DSP channels

Within OpenScape Business, "DSP channels" are used for the conversion (transcoding) of data streams. In principle this is required if there is an IP to TDM or TDM to IP transition for the voice data or if an encryption of the voice data is required. In detail:

30 Max number of 16 simultaneous connection per MOH source

31 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

32 The value depends on UC Suite: System with UC Suite / System without UC Suite

33 Values apply to OpenScape Business as ISDN gateway. G.711 to T38 or vice versa without UC Suite Fax

34 UC Suite can generally handle up to 8 simultaneous fax connections. OpenScape Business X3/X5/X8 as ISDN gateway can process 3 to 12 simultaneous faxes depending on the DSP module. Both parameters in combination determine the number of simultaneous T.38 or G.711 fax connections.

35 Values are staggered according to Voice Channel Booster configuration: with OCCBH or OCCB3 / with OCCBL or OCCB1 / mainboard only

- Voice connection between IP telephone and ISDN or analog (trunk) line.
- Voice connection via IP SIP/ITSP line and internal UP0/E, a/b or ISDN telephones.
- Voice connection from IP line or IP subscriber to an internal conference. Here, a gateway channel is required for each line/IP client involved in a conference.
- Connections from UP0/E, a/b or ISDN phones or ISDN/ analog lines to UC Suite announcements, voicemail, fax or conferences.
- Encrypted voice connections between terminals and encrypted voice connections over ITSP lines. This is not the case for V3 mainboard family, from OpenScape Business V3R4 onward.
- Connections to internal Music on Hold require one DSP channel per configured MoH codec.

For the following connections no DSP channel is needed:

- Connection between internal IP users without encryption (direct payload).
- Connection between ITSP and IP subscriber without encryption.

The DSP channels are realized by a signal processor, which is integrated on the respective OCCL or OCCLA motherboard in the models X1, X3, X5 and X8.

Depending on the type of transcoding, one signal processor can handle more or less DSP channels simultaneously. The following coding (codecs) is supported.

- **For voice connections**
  - Conversion from IP (G.711) to TDM with G.711 or vice versa.
  - Conversion from IP (G.711) to TDM with G.711 or vice versa with encryption (SPE).
  - Conversion from IP (G.729) to TDM with G.711 or vice versa.
  - Conversion from IP (G.729) to TDM with G.711 or vice versa with encryption (SPE).
- **For fax connections**
  - Conversion from T.38 to G.711 when using OpenScape Business as ISDN gateway.
  - Conversion from G.711 Fax to T.38 Fax or vice versa when using the UC-Suite Fax feature.

If the capacity of the signal processor integrated on the mainboard is not sufficient to realize the required number of DSP channels, they can be extended by using the optionally available "Voice Channel Booster" cards OCCBL or OCCBH.

The maximum number of available DSP channels depending on the encoding is shown in Table 11. Please note that each row represents the maximum number of similar DSP channels, but these are dynamically allocated by the system during operation. The number of DSP channels currently occupied during operation can be determined via the OpenScape Business Assistant (WBM). You find further notes about determining the required number of DSP channels in the administration manual.

27.3.2 Details on the use of RTP proxy channels

OpenScape Business uses an internal "RTP proxy" for all VoIP connections via the Internet. The proxy offers a pool of RTP channels that are assigned to the VoIP connections via Internet as follows.

- 1 RTP proxy channel per ITSP call
- 1 RTP proxy channel per Unify Phone call
- 1 RTP proxy channel per system Device @Home in one call
- 1 RTP proxy channel per SIP Device @Home in one call
- 1 RTP proxy channel per myPortal to go VoIP @Home in one call
- 1 RTP proxy channel per myPortal @work VoIP @Home in one call

Within the different OpenScape Business models a different number of RTP proxy channels is available. See Table 44: Expansion Level other functions / resources on page 1373.

Examples

- An external outgoing voice call from an internal IP system subscriber via an ITSP line requires an RTP proxy channel.
- An external voice call from the myPortal to go VoIP Client via internal (campus) WiFi to a subscriber in the public network via an ITSP line requires an RTP proxy channel. This is used for the connection via ITSP to the called subscriber in the public network.
- An external voice call from the myPortal to go VoIP Client via public WiFi to a subscriber in the public network over an ITSP line requires two RTP proxy channels. One RTP proxy channel is required for connecting the VoIP Client to OpenScape Business and another RTP proxy channel for the connection via ITSP to the called subscriber in the public network.
- An external voice call arriving via ITSP to a myPortal @work VoIP Client in the home office requires two RTP proxy channels. One RTP proxy channel is required for the connection from the ITSP to the OpenScape Business system and another one for the connection from OpenScape Business via Internet to the myPortal @work VoIP Client in the home office.

27.4 Maximum values for features

The maximum values described here are mainly based on the software capacities of OpenScape Business.

27.4.1 Connection to Service Provider

	X1W/R		X3W/R		X5W/R		X8W/R		Server (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
ITSP (Internet Telephony Service Provider) connection									
SIP trunk channels	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	
Simultaneous activated ITSP	8	8	8	8	8	8	8	8	8
Routes									
Routes	16	16	16	16	16	16	16	16	16
Overflow routes per route	1	1	1	1	1	1	1	1	1

27.4.2 Stations

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Station number / DID number					
Digits per station number/DID number	16 (default = 3)	16 (default = 3)	16 (default = 3)	16 (default = 3)	16 (default = 3)

27.4.3 UC Smart Expansion Levels

- Expansion levels with V2 OCC mainboards can be found in Table 45: Expansion Level UC Smart with OCCx mainboards on page 1377
- Expansion levels with V3 OCC mainboards can be found in Table 46: Expansion Level UC Smart with OCCSB/R, OCCMA/B or OCCLA mainboards on page 1378
- Expansion levels with OpenScape Business S Server systems can be found in Table 47: Expansion Level UC Smart with OpenScape Business S on page 1380

Table 45: Expansion Level UC Smart with OCCx mainboards

	X1	X3W/R	X5W/R	X8
UC Smart User maximum				
Max number of UC Smart user (Accounts)	30	250/ 150/ 50[36]	250/ 150/ 50[36]	250/ 150/ 50[36]
UC Smart Clients				
Number of simultaneous active UC clients.[37]	30	500/ 300/ 150[36]	500/ 300/ 150[36]	500/ 300/ 150[36]
myPortal @work	30	250/ 150/ 50[36]	250/ 150/ 50[36]	250/ 150/ 50[36]
myPortal @work Parallel calls from VoIP to other called parties[38]	20	30	30	30
myPortal to go[38]	30	150/ 150/ 50[36]	150/ 150/ 50[36]	150/ 150/ 50[36]

	X1	X3W/R	X5W/R	X8
Deskphone CP 400/600/600E/ 700/700X/710 (UC-mode)	30	250/ 150/ 50[36]	250/ 150/ 50[36]	250/ 150/ 50[36]
OpenScape Business Attendant	8	8	8	8
Presence Status				
Status per user	9	9	9	9
Voicemail announcements per presence status	1	1	1	1
Favorites				
Favorites per user	100	100	100	100
Favorites groups per user	10	10	10	10
Call Journal				
Call journal entries per user	100	100	100	100
UC Smart Managed Conference (via UC Client)				
Number of managed conferences	5	5	5	5
Number of users per managed conference	16	16	16	16
Channels for managed conferences	30	30	30	30

Table 46: Expansion Level UC Smart with OCCSB/R, OCCMA/B or OCCLA mainboards

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Smart User maximum								
Max number of UC Smart user (Accounts)	150	150	150/ 500[40]	150/ 500[40]	150/ 500[40]	150/ 500[40]	500	500
UC Smart Clients								

36 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

37 Sum of: myPortal @work, myPortal to go, CP 400/600/600E/700/700X/710 UC mode, Application Launcher, Business Attendant, TAPI 120 (WSI), 3rd-party WSI Clients (Background: Several clients with the same UC Smart Account can log on to the system)

38 The number of simultaneous VoIP connections of the subscriber depends on:

1) the DSP channels available in the system for gateway calls (IP/TDM transition).

2) the internal RTP proxy channels available in the system for VoIP calls via the Internet.

39 The number of simultaneous connections depending on the DSP channels available in the system for gateway calls (IP/TDM transition).

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Number of simultaneous active UC clients.[37]	150	150	150/ 500[40]	300 / 1000	150/ 500[40]	300/ 1000[40]	1000	1000
myPortal @work	150	150	150/ 250[40]	150/ 250[40]	150/ 250[40]	150/ 250[40]	250	250
myPortal @work Parallel calls from VoIP to other called parties[38]	150	150	30/ 70[40]	30/ 70[40]	30/ 70[40]	30/ 70[40]	70	70
myPortal to go[38]	150	150	150/ 500[40]	150/ 500[40]	150/ 500[40]	150/ 500[40]	500	500
myPortal for Teams	150	150	150/ 500[40]	150/ 500[40]	150/ 500[40]	150/ 500[40]	500	500
Deskphone CP 400/600/600E/ 700/700X/710 (UC-mode)	150	150	150/ 500[40]	150/ 500[40]	150/ 500[40]	150/ 500[40]	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
Presence Status								
Status per user	9	9	9	9	9	9	9	9
Voicemail announcements per presence status	1	1	1	1	1	1	1	1
Favorites								
Favorites per user	100	100	100	100	100	100	100	100
Favorites groups per user	10	10	10	10	10	10	10	10
Call Journal								
Call journal entries per user	100	100	100	100	100	100	100	100
UC Smart Managed Conference (via UC Client)								
Number of managed conferences	5	5	5	5	5	5	5	5
Number of users per managed conference	16	16	16	16	16	16	16	16

	X1W/R		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Channels for managed conferences	30	30	30	30	30	30	30	30

Table 47: Expansion Level UC Smart with OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Smart User maximum			
Max number of UC Smart user (Accounts)	50	500	1500
UC Smart Clients			
Number of simultaneous active UC clients.[37]	50	500	1500
myPortal @work	50	250	500
myPortal to go[38]	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710 (UC-mode)	50	250	500
OpenScape Business Attendant	8	8	8
Presence Status			
Status per user	9	9	9
Voicemail announcements per presence status	1	1	1
Favorites			
Favorites per user	100	100	100
Favorites groups per user	10	10	10
Call Journal			
Call journal entries per user	100	100	100
UC Smart Managed Conference (via UC Client)			
Number of managed conferences	10	10	10
Number of users per managed conference	16	16	16
Channels for managed conferences	30	30	30

40 Values are staggered according to Board version: Basic/Advanced

27.4.4 Smart Voicemail Expansion Levels

- Expansion levels with V2 OCC mainboards can be found in Table 48: Expansion level Smart Voicemail with OCCx mainboards on page 1381
- Expansion levels with V3 OCC mainboards can be found in Table 49: Expansion level Smart Voicemail with OCCSB/R, OCCMA/B or OCCLA mainboards on page 1381
- Expansion levels with OpenScape Business S Server systems can be found in Table 50: Expansion level Smart Voicemail with OpenScape Business S on page 1382

Table 48: Expansion level Smart Voicemail with OCCx mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
Smart Voicemail					
Smart Voicemail boxes	30	320	320	320	1500
Messages per Voicemail Box	100	100	100	100	100
Recording time per call (minutes)	2	2	2	2	2
Total recording capacity in hours	32	32	32	32	32
Simultaneous Voicemail connections (channels)	10	10	10	10	60
Announcements	16	16	16	16	16
Company/ Auto Attendants	100	100	100	100	100
Company/ Auto Attendants (Simultaneously active)	6	6	6	6	6

Table 49: Expansion level Smart Voicemail with OCCSB/R, OCCMA/B or OCCLA mainboards

	X1W/R		X3W/R	X5W/R		X8		
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail								
Smart Voicemail boxes	320	320	320/ 500[41]	320/ 500[41]	320/ 500[41]	320/ 500[41]	500	500
Messages per Voicemail Box	100	100	100	100	100	100	100	100
Recording time per call (minutes)	2	4	4	4	4	4	4	4
Total recording capacity in hours	32	64	32	64	32	64	32	64
Simultaneous Voicemail connections (channels)	30	30	30	30	30	30	30	30

	X1W/R		X3W/R	X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Announcements	16	16	16	16	16	16	16	16
Company/ Auto Attendants	100	100	100	100	100	100	100	100
Company/ Auto Attendants (Simultaneously active)	6	6	6	6	6	6	6	6

Table 50: Expansion level Smart Voicemail with OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Smart Voicemail			
Smart Voicemail boxes	1500	1500	1500
Messages per Voicemail Box	100	100	100
Recording time per call (minutes)	4	4	4
Total recording capacity in hours	64	64	64
Simultaneous Voicemail connections (channels)	60	60	60
Announcements	16	16	16
Company/ Auto Attendants	100	100	100
Company/ Auto Attendants (Simultaneously active)	6	6	6

27.4.5 UC Suite Expansion Levels

- Expansion levels with V2 OCC mainboards can be found in Table 51: Expansion Level UC Suite with V2 mainboards on page 1382
- Expansion levels with V3 OCC mainboards can be found in Table 52: Expansion Level UC Suite with OCCSB, OCCMA/B or OCCLA mainboards on page 1385
- Expansion levels with OpenScape Business S Server systems can be found in Table 53: Expansion Level UC Suite with OpenScape Business S on page 1389

Table 51: Expansion Level UC Suite with V2 mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
UC Suite User maximum					

41 Values are staggered according to Board version: Basic/Advanced

	X1	X3W/R	X5W/R	X8	Server (S)
Max number of UC Suite user (Accounts)	-	250/ 150/ 0[42]	250/ 150/ 0[42]	250/ 150/ 0[42]	1500
UC Suite Clients					
Number of simultaneous active UC clients.[43]	-	500/ 150/ 0[42]	500/ 150/ 0[42]	500/ 150/ 0[42]	1500
myPortal for Desktop	-	500/ 150/ 0[42]	500/ 150/ 0[42]	500/ 150/ 0[42]	1500
myPortal for Outlook	-	500/ 150/ 0[42]	500/ 150/ 0[42]	500/ 150/ 0[42]	1500
myAgent (simultaneous active)	-	64	64	64	64
myAgent (configurable)	-	192	192	192	192
myReports	-	1	1	1	1
myAttendant	-	20	20	20	20
myPortal @work	-	250/ 150/ 0[42]	250/ 150/ 0[42]	250/ 150/ 0[42]	250
myPortal @work Parallel calls from VoIP to other called parties[45]	-	30	30	30	60
myPortal to go[45]	-	150/ 150/ 0[42]	150/ 150/ 0[42]	150/ 150/ 0[42]	250
Deskphone 400/600/600E/700/700X/710	-	250/ 150/ 0[42]	250/ 150/ 0[42]	250/ 150/ 0[42]	250
OpenScape Business Attendant	-	8	8	8	8
Presence Status					
Status per UC Suite subscriber	-	9	9	9	9
Voicemail announcements per presence status	-	1	1	1	1
Call Journals (myPortal for Desktop / myPortal for Outlook)					
Archiving duration in the UC clients (days)	-	30 default = 30	30 default = 30	30 default = 30	30 default = 30
Archiving duration in the communication system	-	365 default = 30	365 default = 30	365 default = 30	365 default = 30
Call journal entries[47]	-	Unrestricted[47]	Unrestricted[47]	Unrestricted[47]	Unrestricted[47]
Call journal entries myPortal for Desktop modern GUI	-	100 after startup >100 during operation	100 after startup >100 during operation	100 after startup >100 during operation	100 after startup >100 during operation

	X1	X3W/R	X5W/R	X8	Server (S)
UC Suite Voicemail					
VM boxes	-	500/ 500/ 0[46]	500/ 500/ 0[46]	500/ 500/ 0[46]	1500
VM groups	-	20/ 20/ 0	20/ 20/ 0	20/ 20/ 0	20
Messages per voicemail box[47]	-	n/a	n/a	n/a	n/a
Recording length per call (minutes)	-	15	15	15	15
Recording length which can be forwarded by e-mail (minutes)[48]	-	~10	~10	~10	~10
Total recording capacity (hours)[47]	-	n/a	n/a	n/a	n/a
Simultaneous connections to voicemail (MEB-channels)	-	30	30	30	60
UC Suite AutoAttendant					
Personal Auto Attendant	-	20/ 20/ 0[42]	20/ 20/ 0[42]	20/ 20/ 0[42]	20
Company Auto Attendant	-	1/ 1/ 0[42]	1/ 1/ 0[42]	1/ 1/ 0[42]	1
Multi user Chat (Instant messaging)					
Internal communication partner	-	unrestricited	unrestricited	unrestricited	unrestricited
External communication partner (XMPP)	-	-	-	-	-
Announcements per UC Suite user					
Greeting announcements	-	1/ 1/ 0[42]	1/ 1/ 0[42]	1/ 1/ 0[42]	1
Presence status based announcements	-	1/ 1/ 0[42]	1/ 1/ 0[42]	1/ 1/ 0[42]	1
Personal Auto Attendant announcement	-	1/ 1/ 0[42]	1/ 1/ 0[42]	1/ 1/ 0[42]	1
UC Suite Call Recording					
Recording length per call/ conference	-	Limited by length of call	Limited by length of call	Limited by length of call	Limited by length of call
UC Suite Fax					
Fax boxes	-	500/ 150/ 0[42]	500/ 150/ 0[42]	500/ 150/ 0[42]	1500
Fax box groups	-	60/ 60/ 0[42]	60/ 60/ 0[42]	60/ 60/ 0[42]	60
Stations per Fax box group	-	10/ 10/ 0[42]	10/ 10/ 0[42]	10/ 10/ 0[42]	10
Fax length in pages	-	500/ 500/ 0[42]	500/ 500/ 0[42]	500/ 500/ 0[42]	500

	X1	X3W/R	X5W/R	X8	Server (S)
Simultaneous T.38 Faxes	-	8/ 3/ 0[42]	8/ 3/ 0[42]	8/ 3/ 0[42]	8
Fax merge recipients	-	unrestricted	unrestricted	unrestricted	unrestricted
UC Suite Conferences					
Simultaneous UC Suite Conferences	-	5/ 5/ 0[42]	5/ 5/ 0[42]	5/ 5/ 0[42]	10
Participants per UC Suite Conference	-	16/ 16/ 0[42]	16/ 16/ 0[42]	16/ 16/ 0[42]	16
External participants Users per UC Suite Conference	-	15/ 15/ 0[42]	15/ 15/ 0[42]	15/ 15/ 0[42]	15
Max. Number of channels for UC Suite Conferences	-	30/ 30/ 0[42]	30/ 30/ 0[42]	30/ 30/ 0[42]	60
Number of channels reserved for UC Suite Ad Hoc and Meet Me Conferences	-	20/ 20/ 0[42]	20/ 20/ 0[42]	20/ 20/ 0[42]	60
External database connectivity (LDAP)					
External database connections of UC Server	-	10/ 10/ 0[42]	10/ 10/ 0[42]	10/ 10/ 0[42]	10

Table 52: Expansion Level UC Suite with OCCSB, OCCMA/B or OCCLA mainboards

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Suite User maximum						

42 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

43 Sum of: 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: Several clients with the same UC Suite account can log on to the system)

44 The lower value applies to systems with UC Suite Contact Center

45 The number of simultaneous VoIP connections of the subscriber depends on

1) the DSP channels available in the system for gateway calls (IP/TDM transition).

2) the internal RTP proxy channels available in the system for VoIP calls via the Internet.

46 The UC Booster Card supports a maximum of 500 voicemail boxes, regardless of the UC Suite client limit (150 users).

47 The value depends on the available hard disk HD / SSD storage capacity. A subscriber-related limitation is not implemented.

1) Voicemail / Recordings: One minute recording times uses about 1MB storage space

2) Fax: A standard fax (2 DIN A4 pages) corresponds to approx. 48 KB of storage space)

Example: The storage volume of the partition for recording voice announcements, voicemails, voice calls and faxes is 20 GB for a 160 GB hard drive. This corresponds to a total recording time of about 20000 minutes.

48 In case of longer recordings the recording is split and send in multiple files.

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Max number of UC Suite user (Accounts)	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49]	-	500 300 in case of Contact Center
UC Suite Clients						
Number of simultaneous active UC clients.[43]	-	100/ 1000[49] 600 in case of Contact Center	-	100/ 1000[49] 600 in case of Contact Center	-	1000 600 in case of Contact Center
myPortal for Desktop	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49] 300 in case of Contact Center	-	500 300 in case of Contact Center
myPortal for Outlook	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49] 300 in case of Contact Center	-	500 300 in case of Contact Center
myAgent (simultaneous active)	-	0/ 64[49]	-	0/ 64[49]	-	64
myAgent (configurable)	-	0/ 192[49]	-	0/ 192[49]	-	192
myReports	-	0/ 1[49]	-	0/ 1[49]	-	1
myAttendant	-	4/ 20[49]	-	4/ 20[49]	-	20
myPortal @work	-	50/ 250[49] 300 in case of Contact Center	-	50/ 250[49] 300 in case of Contact Center	-	250 300 in case of Contact Center
myPortal @work Parallel calls from VoIP to other called parties[45]	-	30/ 70[49]	-	30/ 70[49]	-	70
myPortal to go[45]	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49] 300 in case of Contact Center	-	500 300 in case of Contact Center
myPortal for Teams	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49] 300 in case of Contact Center	-	500 300 in case of Contact Center

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Deskphone CP 400/600/600E/ 700/700X/710	-	50/ 500[49] 300 in case of Contact Center	-	50/ 500[49] 300 in case of Contact Center	-	500 300 in case of Contact Center
OpenScape Business Attendant	-	8	-	8	-	8
Presence Status						
Status per UC Suite subscriber	-	9	-	9	-	9
Voicemail announcements per presence status	-	1	-	1	-	1
Call Journals (myPortal for Desktop / myPortal for Outlook)						
Archiving duration in the UC clients (days)	-	30 default = 30	-	30 default = 30	-	30 default = 30
Archiving duration in the communication system	-	365 default = 30	-	365 default = 30	-	365 default = 30
Call journal entries[47]	-	Unrestricted[47]	-	Unrestricted[47]	-	Unrestricted[47]
Call journal entries myPortal for Desktop modern GUI	-	100 after startup >100 during operation	-	100 after startup >100 during operation	-	100 after startup >100 during operation
UC Suite Voicemail						
VM boxes	-	50/ 500[49]	-	50/ 500[49]	-	500
VM groups	-	32	-	32	-	32
Messages per voicemail box[47]	-	n/a	-	n/a	-	n/a
Recording length per call (minutes)	-	15	-	15	-	15
Recording length which can be forwarded by e-mail (minutes)[48]	-	~10	-	~10	-	~10
Total recording capacity (hours)[47]	-	n/a	-	n/a	-	n/a
Simultaneous connections to voicemail (MEB-channels)	-	30/ 60[49]	-	30/ 60[49]	-	60
UC Suite AutoAttendant						

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Personal Auto Attendant	-	20	-	20	-	20
Company Auto Attendant	-	1	-	1	-	1
Multi user Chat (Instant messaging)						
Internal communication partner	-	unrestricited	-	unrestricited	-	unrestricited
Announcements per UC Suite user						
Greeting announcements	-	1	-	1	-	1
Presence status based announcements	-	1	-	1	-	1
Personal Auto Attendant announcement	-	1	-	1	-	1
UC Suite Call Recording						
Recording length per call/ conference	-	Limited by length of call	-	Limited by length of call	-	Limited by length of call
UC Suite Fax						
Fax boxes	-	50/ 500[49]	-	50/ 500[49]	-	500
Fax box groups	-	60	-	60	-	60
Stations per Fax box group	-	10	-	10	-	10
Fax length in pages	-	500	-	500	-	500
Simultaneous T.38 Faxes	-	3/ 8[49]	-	3/ 8[49]	-	8
Fax merge recipients	-	unrestricted	-	unrestricted	-	unrestricted
UC Suite Conferences						
Simultaneous UC Suite Conferences	-	5	-	5	-	5
Participants per UC Suite Conference	-	16	-	16	-	16
External participants Users per UC Suite Conference	-	15	-	15	-	15
Max. Number of channels for UC Suite Conferences	-	30	-	30	-	30
Number of channels reserved for UC Suite Ad Hoc and Meet Me Conferences	-	20	-	20	-	20

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
External database connectivity (LDAP)						
External database connections of UC Server	-	10	-	10	-	10

Table 53: Expansion Level UC Suite with OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Suite User maximum			
Max number of UC Suite user (Accounts)	150	500	1500
UC Suite Clients			
Number of simultaneous active UC clients.[43]	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (simultaneous active)	0	64	64
myAgent (configurable)	0	192	192
myReports	1	1	1
myAttendant	20	20	20
myPortal @work	50	250	500
myPortal @work Parallel calls from VoIP to other called parties[45]	30	60	60
myPortal to go[45]	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
Presence Status			
Status per UC Suite subscriber	9	9	9

49 Values are staggered according to Board version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Voicemail announcements per presence status	1	1	1
Call Journals (myPortal for Desktop / myPortal for Outlook)			
Archiving duration in the UC clients (days)	30 default = 30	30 default = 30	30 default = 30
Archiving duration in the communication system	365 default = 30	365 default = 30	365 default = 30
Call journal entries[47]	Unrestricted[47]	Unrestricted[47]	Unrestricted[47]
Call journal entries myPortal for Desktop modern GUI	100 after startup >100 during operation	100 after startup >100 during operation	100 after startup >100 during operation
UC Suite Voicemail			
VM boxes	150	500	1500
VM groups	32	32	32
Messages per voicemail box[47]	n/a	n/a	n/a
Recording length per call (minutes)	15	15	15
Recording length which can be forwarded by e-mail (minutes)[48]	~10	~10	~10
Total recording capacity (hours)[47]	n/a	n/a	n/a
Simultaneous connections to voicemail (MEB-channels)	60	60	60
UC Suite AutoAttendant			
Personal Auto Attendant	20	20	20
Company Auto Attendant	1	1	1
Multi user Chat (Instant messaging)			
Internal communication partner	unrestricited	unrestricited	unrestricited
Announcements per UC Suite user			
Greeting announcements	1	1	1
Presence status based announcements	1	1	1
Personal Auto Attendant announcement	1	1	1
UC Suite Call Recording			
Recording length per call/ conference	Limited by length of call	Limited by length of call	Limited by length of call
UC Suite Fax			
Fax boxes	1500	1500	1500
Fax box groups	60	60	60

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Stations per Fax box group	10	10	10
Fax length in pages	500	500	500
Simultaneous T.38 Faxes	8	8	8
Fax merge recipients	unrestricted	unrestricted	unrestricted
UC Suite Conferences			
Simultaneous UC Suite Conferences	10	10	10
Participants per UC Suite Conference	16	16	16
External participants Users per UC Suite Conference	15	15	15
Max. Number of channels for UC Suite Conferences	60	60	60
Number of channels reserved for UC Suite Ad Hoc and Meet Me Conferences	60	60	60
External database connectivity (LDAP)			
External database connections of UC Server	10	10	10

27.4.6 Functions at the Telephone

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Caller List for system (HFA) phones					
Caller lists per system	650	650	650	650	1300
Caller lists per station in the system	1	1	1	1	1
Entries per caller list	10	10	10	10	10
Saved digits per entry plus seizure code	25 + (6)	25 + (6)	25 + (6)	25 + (6)	25 + (6)
Direct Stations Keys (DSS keys)					
Key modules per communication system	250	250	250	250	250
Key modules per telephone	2	2	2	2	2
Keys per OpenStage key module	12	12	12	12	12
Keys per OpenStage key module 15	18	18	18	18	18
Busy Lamp Fields (BLF) per communication system	12	25	25	25	25
Keys per Busy Lamp Field	90	90	90	90	90

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Individual Speed Dialing (ISD)					
Entries in the KWI pool per communication system	2000	2000	2000	2000	2000
Entries per station	10	10	10	10	10
Digits per entry (plus seizure code)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
System Speed Dialing (SSD)					
Entries in the KWI pool per communication system	8000	8000	8000	8000	8000
Character length of name	16	16	16	16	16
Digits per entry (plus seizure code)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Redialing					
Entries per OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3	3
Entries per OpenStage 15	10	10	10	10	10
Entries per OpenStage 60/ 60G/ 80/ 80G	30	30	30	30	30
Entries per telephone without display	1	1	1	1	1
Saved digits per entry	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Call waiting / call waiting tones					
Waiting caller per telephone	16				
Parking					
Parking Positions per system	10				
Callback calls					
Callback entries per telephone	5				
Advisory messages / Message texts					
Advisory messages per system	250	250	250	250	250
Message texts per system	150	150	150	150	150
Configurable advisory messages + message texts per system	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10
Character length of a configurable advisory message/ message text	24	24	24	24	24

	X1W/R	X3W/R	X5W/R	X8W/R	Server (S)
Received advisory message/ message texts per telephone with display	5	5	5	5	5
Received advisory message/ message texts per telephone without display	1	1	1	1	1
Ringing group on					
Stations included	5				
Call Forwarding (CF)					
FWD destinations per telephone	4	4	4	4	4
Digits per external CFW destination (plus seizure code)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Chained FWD destinations					5
System controlled conferences					
Simultaneous system conferences per system	10	10	10	10	8
Participants per conference	8	8	8	8	8
External participants per conference	7	7	7	7	7
Conference channels	32	32	32	32	20
Entrance Telephone/Door Opener					
Connections via a/b interfaces per system	4	4	4	4	-
Digits per code entry	5	5	5	5	-
Trunk queuing					
Simultaneous entries per system	32	32	32	32	-

NOTICE: For all the above call forwarding scenarios, users can enter only one forwarding destination per MSN. A total of 10 multiple subscriber numbers can be forwarded.

In case of ITSP or ISDN configured with DID, this number is 249.

27.4.7 Working in a Team (Groups)

- Information on V2 OCC mainboards can be found in Table 54: Data for V2 mainboards on page 1394
- Information on V3 OCC mainboards can be found in Table 55: Data for V3 mainboards on page 1395

- Information on OpenScape Business S Server systems can be found in Table 56: Data for OpenScape Business S on page 1397

Table 54: Data for V2 mainboards

	X1	X3W/R	X5W/R	X8
Call Pickup groups				
Call pickup groups per system	32	32	32	32
Stations per call pickup group	32	32	32	32
Call Ringing (user configurable group)				
Number of extensions in call ringing group	5	5	5	5
Group calls, hunt groups, Basic MULAPs				
Total of group calls, hunt groups, Basic MULAPs, Executive MULAPs and voicemail groups per communication system	800	800	800	800
Length of group name	16	16	16	16
Number of groups to which a user can be assigned	32	32	32	32
Subscribers per group call, hunt group, Basic MULAP	20	20	20	20
Executive MULAPs, Team groups, Top groups and voicemail groups:				
Total number of Executive MULAP-, Team-and Top groups per	500	500	500	500
Subscribers per Executive MULAP, Team group, Top group	10	10	10	10
MULAP keys per telephone	10	10	10	10
Voicemail groups				
Number of Voicemail groups	20	20	20	20
Stations per voicemail group	20	20	20	20
Internal paging (Voice Paging)				
Simultaneous announcements per communication system	1	1	1	1
Recipients of the announcement	20	20	20	20
UCD groups				
UCD groups per system	60	60	60	60
Announcements per UCD group	7	7	7	7
Priority levels per UCD group	10	10	10	10
Queued calls per UCD group (last group max 72)	30	30	30	30
UCD agents				

	X1	X3W/R	X5W/R	X8
UCD agent IDs per communication system	330	330	330	330
Simultaneously active UCD agents per communication system	64	64	64	64
UCD Announcements				
Number of callers, per communication system, for whom an announcement can be simultaneously played	8	8	8	8

Table 55: Data for V3 mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Call Pickup groups								
Call pickup groups per system	64	64	64/128[50]	64/128[50]	64/128[50]	64/128[50]	128	128
Stations per call pickup group	32	32	32	32	32	32	32	32
Call Ringing (user configurable group)								
Number of extensions in call ringing group	5	5	5	5	5	5	5	5
Group calls, hunt groups, Basic MULAPs								
Total of group calls, hunt groups, Basic MULAPs, Executive MULAPs and voicemail groups per communication system	800	800	800	800	800	800	800	800
Length of group name	16	16	16	16	16	16	16	16
Number of groups to which a user can be assigned	32	32	32	32	32	32	32	32
Subscribers per group call, hunt group, Basic MULAP	20	20	20/32[50]	20/32[50]	20/32[50]	20/32[50]	32	32
Executive MULAPs, Team groups, Top groups and voicemail groups:								
Total number of Executive MULAP-, Team-and Top groups per	500	500	500	500	500	500	500	500

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Subscribers per Executive MULAP, Team group, Top group	10	10	10	10	10	10	10	10
MULAP keys per telephone	10	10	10	10	10	10	10	10
Voicemail groups								
Number of Voicemail groups	20	20	20	20	20	20	20	20
Stations per voicemail group	20	20	20	20	20	20	20	20
Internal paging (Voice Paging)								
Simultaneous announcements per communication system	1	1	1	1	1	1	1	1
Recipients of the announcement	20	20	20/32[50]	20/32[50]	20/32[50]	20/32[50]	32	32
UCD groups								
UCD groups per system	60	60	60	60	60	60	60	60
Announcements per UCD group	7	7	7	7	7	7	7	7
Priority levels per UCD group	10	10	10	10	10	10	10	10
Queued calls per UCD group (last group max 72)	30	30	30	30	30	30	30	30
UCD agents								
UCD agent IDs per communication system	330	330	330	330	330	330	330	330
Simultaneously active UCD agents per communication system	64	64	64	64	64	64	64	64
UCD Announcements								
Number of callers, per communication system, for whom an announcement can be simultaneously played	8	8	8	8	8	8	8	8

Table 56: Data for OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Call Pickup groups			
Call pickup groups per system	32	64	128
Stations per call pickup group	32	32	32
Call Ringing (user configurable group)			
Number of extensions in call ringing group	5	5	5
Group calls, hunt groups, Basic MULAPs			
Total of group calls, hunt groups, Basic MULAPs, Executive MULAPs and voicemail groups per communication system	800	800	800
Length of group name	16	16	16
Number of groups to which a user can be assigned	32	32	32
Subscribers per group call, hunt group, Basic MULAP	32	32	32
Executive MULAPs, Team groups, Top groups and voicemail groups:			
Total number of Executive MULAP-, Team- and Top groups per	500	500	500
Subscribers per Executive MULAP, Team group, Top group	10	10	10
MULAP keys per telephone	10	10	10
Voicemail groups			
Number of Voicemail groups	20	20	20
Stations per voicemail group	20	20	20
Internal paging (Voice Paging)			
Simultaneous announcements per communication system	1	1	1
Recipients of the announcement	20	20	20
UCD groups			
UCD groups per system	60	60	60
Announcements per UCD group	7	7	7
Priority levels per UCD group	10	10	10
Queued calls per UCD group (last group max 72)	30	30	30
UCD agents			

50 Values are staggered according to Board version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UCD agent IDs per communication system	330	330	330
Simultaneously active UCD agents per communication system	64	64	64
UCD Announcements			
Number of callers, per communication system, for whom an announcement can be simultaneously played	8	8	8

27.4.8 Call Routing

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Least Cost Routing LCR					
Dialed digits	24	24	24	24	24
Verified digits	24	24	24	24	24
Dial Plans (max 10 field per plan)	1000	1000	1000	1000	1000
Route tables	254	254	254	254	254
Routes per routing table	16	16	16	16	16
Dial rules per route	254	254	254	254	254
Number of time zones per day/week	8	8	8	8	8
Digits per dial rule	40	40	40	40	40
Night Service					
Authorized stations per system	5	5	5	5	5
E911 Emergency Call Service (for the U.S. only)					
Digits per LIN (Location Identification Number)	16	16	16	16	16
Hotline after Timeout/Hotline					
Hotline destinations per communication system	6	6	6	6	6
CON groups					
CON groups per system	64	64	64	64	64

Attendants for V2 mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant					

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant (UC Suite) per system	-	20	20	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Auto Attendant	-	20/ 20/ 0[51]	20/ 20/ 0[51]	20/ 20/ 0[51]	20
OpenScape Business Attendant					
OpenScape Business Attendants per system	-	8	8	8	8

Attendants for V3 mainboards

	X1W/R	X3W/R	X5W/R	X8	Server (S)
myAttendant					
myAttendant (UC Suite) per system	4	4/20[52]	4/20[52]	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Auto Attendant	20	20/ 20/[52]	20/ 20[52]	20/ 20[52]	20
OpenScape Business Attendant					
OpenScape Business Attendants per system	8	8	8	8	8

27.4.9 Multimedia Contact Center

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Contact Center Queues					
Queues per communication system	-	50	50	50	50
Wrap Up					
Wrap up codes	-	unrestricted	unrestricted	unrestricted	unrestricted
Agents					
Agents simultaneous active)	-	64	64	64	64
Agents (configurable)	-	192	192	192	192

51 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster. For V3 mainboards, the hightest value is valid.

52 Values are staggered according to Board version: Basic/Advanced

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Historical Reporting					
myReports Cients simultaneously active per System	-	1	1	1	1

27.4.10 Mobility Expansion Limits

Table 57: Data for V2 OCC mainboards

	X1	X3W/R	X5W/R	X8
Teleworker workplaces				
Teleworker workplaces via VPN per communication system	10	10	10	10
Mobility Stations				
Mobility Entry stations per system	30	150	150	150
myPortal to go (UC Smart): stations per system	30	150/ 150/ 50[53]	150/ 150/ 50[53]	150/ 150/ 50[53]
myPortal to go (UC Suite): stations per system	-	150/ 150/ 0[53]	150/ 150/ 0[53]	150/ 150/ 0[53]

Table 58: Data for V3 OCC mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teleworker workplaces								
Teleworker workplaces via VPN per communication system	10	10	10	10	10	10	10	10
Mobility Stations								
Mobility Entry stations per system	150/ 500[54]	150/ 500[54]	150	150/ 500[54]	150/ 500[54]	150/ 500[54]	500	500
myPortal to go (UC Smart): stations per system	150	150	150/ 500[54]	150/ 500[54]	150/ 500[54]	150/ 500[54]	500	500

53 Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal to go (UC Suite): stations per system	-	50	-	50/ 500 300 in case of Contact Center	-	50/ 500 300 in case of Contact Center	-	500 300 in case of Contact Center
myPortal for Teams (UC Smart): stations per system	150	150	150/ 500[54]	150/ 500[54]	150/ 500[54]	150/ 500[54]	500	500
myPortal for Teams (UC Suite): stations per system	-	50	-	50/ 500 300 in case of Contact Center	-	50/ 500 300 in case of Contact Center	-	500 300 in case of Contact Center

Table 59: Data for OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Mobility Stations			
Mobility Entry stations per system	50	150	150
myPortal to go (UC Smart): stations per system	50	250	500
myPortal to go (UC Suite): stations per system	50	250	500
myPortal for Teams (UC Smart): stations per system	50	250	500
myPortal for Teams (UC Suite): stations per system	50	250	500

27.4.11 Security

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Individual lock code					
Digits per phone lock code	5	5	5	5	5
Permitted characters	0 - 9	0 – 9	0 – 9	0 – 9	0 – 9
Toll restriction					
Number of allowed lists	6	6	6	6	6
Number of denied lists	6	6	6	6	6

54 Values are staggered according to Board version: Basic/Advanced

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Allowed list, short (10 entries with 32 digits each)	5	5	5	5	5
Allowed list, long (100 entries with 32 digits each)	1	1	1	1	1
Denied list, short (10 entries with 32 digits each)	5	5	5	5	5
Denied list, long (50 entries with 32 digits each)	1	1	1	1	1
Classes of Service					
Classes of Service per system	15	15	15	15	15
Matrix size – day and night – number of trunks	30	30	30	30	30
Allowed and denied lists	15	15	15	15	15
Closed used groups (ITR groups – VBZ Gruppen)					
ITR groups per system	16	64	64	64	64
Matrix size – day and night – number of trunks	30	30	30	30	30
Allowed and denied lists	15	15	15	15	15

27.4.12 Networking OpenScape Business

Networking OpenScape Business X1W/R, OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S: Project-specific releases can be requested for networking requirements beyond the configuration limits listed here. Please also refer to the current Sales Release.

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Networking OpenScape Business					
Networked communication systems (nodes)	8/ 32[55]	8/ 32[55]	8/ 32[55]	8/ 32[55]	8/ 32[55]
Stations in the network	1000	1000	1000	1000	1000

[55] Values are staggered according to: Network with UC Suite / Network without UC Suite

27.4.13 Application Connectivity

Table 60: Data for V2 OCC mainboards

	X1	X3W/R	X5W/R	X8
CSTA Interface				
CSTA links via CSP per system	-	4/ 4/ 0[56]	4/ 4/ 0[56]	4/ 4/ 0[56]
Monitor points for trunks or stations	-	1500	1500	1500
TAPI 170 middleware server	-	4	4	4
TAPI 120 clients (CSTA)	-	150/ 150/ 0[56]	150/ 150/ 0[56]	150/ 150/ 0[56]
Web Services Interface (WSI)				
WSI - simultaneous active clients in sum	30	500/ 300/ 150[56]	500/ 300/ 150[56]	500/ 300/ 150[56]
myPortal @work	30	250/ 150/ 50[56]	250/ 150/ 50[56]	250/ 150/ 50[56]
myPortal to go	30	150/ 150/ 50[56]	150/ 150/ 50[56]	150/ 150/ 50[56]
DeskPhone CP 400/600/600E/ 700/700X/710 with WSI	30	150/ 150/ 50[56]	150/ 150/ 50[56]	150/ 150/ 50[56]
OpenScape Business Attendant	0	8/ 8/ 8[56]	8/ 8/ 8[56]	8/ 8/ 8[56]
OpenScape Business BLF	0	150/ 150/ 50[56]	150/ 150/ 50[56]	150/ 150/ 50[56]
Application Launcher	30	250/ 150/ 50[56]	250/ 150/ 50[56]	250/ 150/ 50[56]
TAPI 120 (WSI mode)	30	0/ 0/ 30[56]	0/ 0/ 30[56]	0/ 0/ 30[56]
3rd party application	rest	rest	rest	rest

Table 61: Data for V3 OCC mainboards

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
CSTA Interface								
CSTA links via CSP per system	-	-	4	4	4	4	4	4
Monitor points for trunks or stations	1650	1650	1650/ 3750[57]	1650/ 3750[57]	1650/ 3750[57]	1650/ 3750[57]	3750	3750
TAPI 170 middleware server	4	4	4	4	4	4	4	4

[56] Values are staggered according to UC Booster configuration: Booster Server / Booster Card / without UC Booster

	X1W/R		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
TAPI 120 clients (CSTA)	150	150	150/ 500[57]	150/ 500[57]	150/ 500[57]	150/ 500[57]	500	500
Web Services Interface (WSI)								
WSI - simultaneous active clients in sum	150	300	150/ 500[57]	300/ 1000[57]	150/ 500[57]	300/ 1000[57]	1000	1000
myPortal @work	150	150	150/ 250[57]	150/ 250[57]	150/ 250[57]	150/ 250[57]	250	250
myPortal to go	150	150	150/ 500[57]	150/ 500[57]	150/ 500[57]	150/ 500[57]	500	500
myPortal for Teams	150	150	150/ 500[57]	150/ 500[57]	150/ 500[57]	150/ 500[57]	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 with WSI	150	150	150/ 500[57]	150/ 500[57]	150/ 500[57]	150/ 500[57]	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[57]	150/ 500[57]	150/ 500[57]	150/ 500[57]	500	500
TAPI 120 (WSI mode)	**NOTICE:** Phased out on V3 OCC mainboards. Supported in V3 only for V2 mainboards.							
3rd party application	rest	rest	rest	rest	rest	rest	rest	rest

Table 62: Data for OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
CSTA Interface			
CSTA links via CSP per system	4	4	4
Monitor points for trunks or stations	3750	3750	3750
TAPI 170 middleware server	4	4	4
TAPI 120 clients (CSTA)	50	500	1500
Web Services Interface (WSI)			

[57] Values are staggered according to Board version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
WSI - simultaneous active clients in sum	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 with WSI	50	250	500
OpenScape Business Attendant	8	8	8
Application Launcher	50	250	500
TAPI 120 (WSI mode)	0	0	0
3rd party application	rest	rest	rest

27.4.14 Accounting

	X1W/R	X3W/R	X5W/R	X8	Server (S)
Call Detail Recording Central					
Entries in the call data buffer per system	20000	20000	20000	20000	20000
Account Code (ACCT):					
Account code entries per communication system	1000	1000	1000	1000	1000
Verifiable digits per Acc. code	11	11	11	11	11
Permitted characters	0-9	0-9	0-9	0-9	0-9

28 Expert mode

Expert mode provides menus and functions to configure and maintain the system.

28.1 Display Conventions for Parameter Descriptions

The parameter descriptions follow the structure of the Expert mode in the WBM.

Menu Item	Each menu item in the Expert mode is associated with a (context-sensitive) help topic that you can call up directly from within the WBM. The title of the Help topics displays the path of the WBM window. Example: **Basic Settings** > **System** > **System Flags**
Tab	Each tab has a separate parameter table in the help topic associated with it. The same parameters of different tabs are described in the same parameter table. About each parameter table is a list of the tab(s) for which the parameters are valid. Example: • **Add Static IP Address** • **Edit Static IP Address** • **Delete Static IP Address**
Area	If the WBM windows are organized into areas, you will find this structure reflected in the parameter table as well. The parameter table will then contain a subheading for each area, followed by the parameters of this area.
Parameters	Parameters are described in a two-column parameter table. The left column contains the parameter names. The right column describes the parameters. Self-explanatory parameters are mentioned, but not described. Value ranges and default values can be found at the end of the description, if any.
Parameter (optional)	Parameters that do not need to be filled are flagged with the keyword "optional".

Entry in drop-down list	Drop-down list items which are not self-explanatory are also listed as named parameters in the left column of the parameter table. The entry is separated by a colon from the name of the drop-down list. Example: **Encryption Algorithms: AES**
Check boxes, Radio buttons and Flags	The descriptions for check boxes, radio buttons and flags always refer to the enabled state.

28.2 Maintenance

The functions for maintaining the communication system, e.g., for uploading Music on Hold or updating software images are grouped together under **Maintenance**.

28.2.1 Configuration

Under **Configuration** you will find a group of functions to load Music on Hold (MoH) or display the hardware configuration, for example.

28.2.1.1 Configuration > Music on Hold (MoH) > Load to Gateway

Parameter Description of Tabs::

- **Load Music on Hold Files via HTTP**

Parameters	Description
Load Music on Hold Files via HTTP	
MoH Day File	Selection of the MoH file for day service from the local file system. File format: see note in WBM.
MoH Night File	Selection of the MoH file for night service from the local file system. File format: see note in WBM.
Load	Loads the selected MoH files into the system (requires a restart). Activation under Setup, Central Telephony > Music on Hold/Announcements.

Parameter Description of Tabs::

- **Load Audio Files via HTTP**

Parameters	Description
Load Audio Files via HTTP	

Parameters	Description
Announcement File	Select the WAV file with the announcement from the local file system. File format: see note in WBM.
Already Uploaded Audio Files	
Wave File	Displays the announcement files loaded in the communication system
Delete	Deletes the announcement file
Load	Loads the selected announcement file into the system. Activation under Setup, Central Telephony> Music on Hold/Announcements.

28.2.1.2 Configuration > Announcements > Load to Gateway

Parameter Description of Tabs:

- **Load Audio Files via HTTP**

Parameters	Description
Load Audio Files via HTTP	
Announcement File	Select the WAV file with the announcement from the local file system. File format: see note in WBM.
Already Uploaded Audio Files	
Wave File	Displays the announcement files loaded in the communication system
Delete	Deletes the announcement file
Load	Loads the selected announcement file into the system. Activation under Setup, Central Telephony> Music on Hold/Announcements.

28.2.1.3 Configuration > Port Configuration

Parameter Description of the Tab:

- **Export Configuration**

Parameters	Description
Export Configuration	
File name	Name of the exported file.

Parameters	Description
Action	Exports a zipped XML file (e.g., for editing in Excel) with the following data: name, phone number of the subscriber, direct inward dialing number, station type, licenses, groups/hunt groups (not team/top), virtual stations, trunks, trunk groups, voicemail. **NOTICE:** Unify Phone users data (groups, licenses, etc.) are not be part of this file to avoid data consistency and prevent configuration issues, in cases where Unify Phone has not been fully implemented or enabled.

28.2.1.4 Configuration > SmartVM

Parameter Description of Tabs:

- **Overview**

Parameters	Description
Languages Displays all languages in which the voice prompts are available. The following naming conventions exist: aabb AA = two-digit language code BB = two-digit country code The country code (bb) is usually identical to the language code (aa).	
Mailbox Information	
Call number	Displays the call number of the voicemail box
Name	Displays the name of the voicemail box.
Messages	Displays the number of new messages / total number of messages.
Total Mailbox usage	Displays the disk space consumption in percent.

28.2.1.5 Configuration > SmartVM > Mailbox Operations

Parameter Description of Tabs:

- **Execute Mailbox Operations**

Parameters	Description
Reset All Mailbox configuration (delete all messages and greetings)	If this flag is enabled, all greetings and messages from all voicemail boxes on the SmartVM are deleted. Default: disabled.
Index	Displays the index of the voicemail box.

Parameters	Description
CallNo	Displays the call number of the voicemail box
Name	Displays the name of the voicemail box.
Reset Passwords	If this flag is enabled, the password of the voicemail box is reset to the default password `123456`. The user must change the password at the next use of the voicemail box. Default: disabled.
Initialize mailboxes	If this flag is enabled, the following actions are performed for the selected voicemail box: Standard Mailboxes: – The password is reset – The **Recording** flag is set – Messages are deleted – Greetings are deleted – Greeting control to manual – Active greeting: Greeting 1 AutoAttendant mailboxes: – The password is reset - The **Intercept after announcem.** flag is disabled – Speed dial destinations are deleted – Greetings are deleted – Greeting control to manual – Active greeting: Greeting 1 Default: disabled.

28.2.1.6 Configuration > SmartVM > File Operations

Parameter Description of Tabs:

- **Backup**

Parameters	Description
Backup	
Messages	If this flag is enabled, messages from the selected voicemail boxes are backed up in addition to the greetings. Default: disabled.
Available Mailboxes	List of all existing voicemail boxes. You can selectively add individual or even all voicemail boxes to the list of voicemail boxes to be backed up.
Mailboxes for backup	List of voicemail boxes to be backed up.

Parameters	Description
Buttons	
Apply	The greetings (and messages if the **Messages** flag was enabled) of the voicemail boxes to be backed up are saved in a backup file (`*.tar`).

Parameter Description of Tabs:

- **Greetings**

Parameters	Description
Greetings	
Mailbox selection	Selects the voicemail box.
Greeting 1 (day)	Displays the greeting currently being used. **Standard** means that no customized greeting is available for the subscriber.
Greeting 2 (night)	Displays the greeting currently being used. **Standard** means that no customized greeting is available for the subscriber.
Greeting 3	Displays the greeting currently being used. **Standard** means that no customized greeting is available for the subscriber.
Greeting 4	Displays the greeting currently being used. **Standard** means that no customized greeting is available for the subscriber.
Buttons	
Browse	Enables navigation to the storage path of the greetings file.
Load	Loads a previously saved greeting or a wave file into the SmartVM. The Wave file to be loaded must have the following format: PCM, 16 Bit, 8kHz, mono The selected Wave file is converted on loading. Depending on the size of the wave file, this may take some time to complete.
backup	The currently used greeting is backed up on the PC. The greeting is saved on the PC in binary format (vma file) and can therefore not be played back or edited.
Delete	The currently used greeting is deleted from the SmartVM.

Parameter Description of Tabs:

- **Restore**

Parameters	Description
Restore	
Messages	Overwrites not only the greetings of the selected mailboxes, but also the messages. Default: disabled.

Parameters	Description
Override	If this flag is disabled, only the greetings of the selected voicemail boxes that are present in the backup data will be overwritten. If the **Messages** flag is also enabled, the messages contained in the backup data are included as well. Existing messages are retained. If this flag is enabled, all the greetings and messages of the selected voicemail boxes in the SmartVM will be deleted before the restore. If voicemail boxes which are not contained in the backup data are selected, these will also be deleted! The greetings contained in the backup data are transferred. If the **Messages** flag is also enabled, the messages contained in the backup data are transferred as well. Default: disabled.
Available mailboxes	List of all existing voicemail boxes in the backup file. You can selectively add individual or even all voicemail boxes to the list of voicemail boxes to be restored.
Mailboxes for backup	List of voicemail boxes to be restored.
Buttons	
Browse	Enables navigation to the storage path of the backup file.
Load	The voicemail boxes contained in the backup file are displayed. On clicking the button again, the greetings and messages of the selected voicemail boxes are restored.

28.2.1.7 Configuration > Branding

Parameter Description of the Tab:

- **Branding**

Parameters	Description
Branding	Selects the product name.

28.2.1.8 Configuration > IP Gateway Address

Parameter Description of the Tab:

- **Change IP gateway address**

Parameters	Description
Change IP gateway address	
Gateway IP address	Entry of the IP address of the communication system, e.g., 192.168.1.2

28.2.2 Software Image

The functions for refreshing the gateway software and the phone images are grouped together under **Software Image**.

28.2.2.1 Software Image > System Software > Update via Internet

Parameter Description of Tabs::

- **Load Software Images from Web Server**

Parameters	Description
Web Server Settings	
Software Image URL	Display and edit the link to the software server, including the path to the image file.
User name	User name for logging into the software server.
Password	Password for logging into the software server.
Software Update Information	Activation of the check to determine whether a new software version has been provided on the software server.
Start Time	Time of the check. Value range: 00.00 to 24.00, default value: 02.00
Use Proxy	Proxy activation, if a proxy is used.
HTTP Proxy	
HTTP Proxy	Input of the link to the proxy server.
HTTP Proxy Port	Input of the port of the proxy server. Default value: 80
User name	User name for logging into the proxy server.
Password	Password for logging into the proxy server.
Use Dedicated Static Route	Customers with a WAN connection for SIP trunks without internet data volume, can use the **Use Dedicated Static Route** functionality to perform an OSBiz software update via alternative LAN interface. The dynamic IP address of the update server is determined automatically and is then available as a routing entry for this process. To use this option: • Activate the flag **Use Dedicated Static Route**
Clean up storage before transfer	Deletes storage files before transferring software images
Dedicated Static Route for Software Update via LAN Interface	
Gateway IP Address of the Route	Configure the IP address of the default gateway of the LAN interface - through which a connection to the Internet is possible - as the Gateway IP address of the route.

Parameters	Description
Last Software Update on	Displays when the last software update was performed.
Buttons	
Default	Resets edited values back to the default values.

28.2.2.2 Software Image > System Software > Update via File Upload

Parameter Description of Tabs:

- **Load Software Images via File Upload**

Parameters	Description
Remote File Name (PC File System)	Navigate to the storage location of the image file.
Clean up storage space before transfer	When the update is run with this flag active, logs, traces, phone software images, and TCP dumps, are deleted to free storage memory.
Software Activation	
Start action immediately after transfer	The software is immediately transferred to the communication system in the background. After two restarts, the software is up-to-date.
Start Action in	The software is immediately transferred to the communication system in the background. After the specified period, the software is activated. Input of the time period in days, hours and minutes.
Start Action on	The software is immediately transferred to the communication system in the background. The software is activated at the specified time. Input of the time as the date and time.
Local System Time	Displays the date and time of the system.
Software version of the currently used system software images	Displays the software version of the current image file.

28.2.2.3 Software Image > System Software > Update via USB Stick

Parameter Description of Tabs::

- **Load Software Images from USB Stick**

Parameters	Description
List of all existing compatible image files	
Version	Displays the version number of the image files found on the USB device.
Load	Selection of the image file found on the USB device to be used for the software update.

Parameters	Description
File name	Displays the file names of the image files found on the USB device.
Size of Image (MB)	Displays the file size of the image files found on the USB device.
Software Activation	
Start action immediately after transfer	The software is transferred immediately to the communication system in the background and activated. System operations are temporarily interrupted for the activation.
Start Action in	The software is immediately transferred to the communication system in the background. After the specified period, the software is activated. Input of the time period in days, hours and minutes.
Start Action on	The software is immediately transferred to the communication system in the background. The software is activated at the specified time. Input of the time with the date and time.
Local System Time	Displays the date and time of the system.
Software version of the currently used system software images	Displays the current software version.

28.2.2.4 Software Image > Phone Images > Load

Parameter Description of Tabs:

- **Load Phone Software**

Parameters	Description
Remote File Name (PC File System)	Selection of the phone software (image file)
Currently installed images	
Delete	The phone images are marked for deletion.
File name	Displays the file name of the image file.
Device type	Displays the system telephone type associated with the image file.
Version	Displays the version of the image file.
Buttons	
Load	The specified phone image is loaded into the communication system.
Delete	The selected phone images are deleted from the communication system.

28.2.2.5 Software Image > Phone Images > Deploy

Parameter Description of Tabs:

- **Deployment of phone software**

Parameters	Description
Currently installed images	
Deploy	If this check box is selected, the phone software is transmitted to all connected system telephones of the telephone type.
File name	Displays the file name of the image file.
Device type	Displays the system telephone type associated with the image file.
Version	Displays the version of the image file.
Type	Type of the system telephone.
Standard	Any phone software flagged as the default will be automatically transferred to any system telephone associated with this type whenever that phone logs into the system for the first time.

28.2.2.6 Software Image > Phone Images > Deploy to device

Parameter Description of Tabs:

- **Deployment of phone software per device**

  If the user is a Deskshare User the check box will be greyed-out, so you cannot deploy a device to that user.

Parameters	Description
Currently installed images	
Call no	Phone number of the system telephone.
Device type	Type of the system telephone.
IP Address	IP address of the system telephone; direct link to the WBM of the system telephone.
MAC Address	MAC address of the system telephone.
Current SW version	Current software version of the system telephone.
Deployable software	Selection of the phone image to be transmitted to the system telephone.

28.2.2.7 Software Image > Phone Image Logos > Load

An image (e.g., a company logo) can be loaded onto the display of the system telephones (OpenStage 40/60/80 or Telekom variants); displayed in the idle state (on-hook). For details on the specification of the logo file, see Telephone Logos .

Parameter Description of Tabs:

- **Loading the Phone logo**

Parameters	Description
Remote File Name (PC File System)	Selection of the file with the phone logo.
Currently Installed Logo Images	
Delete	The phone logo files are marked for deletion.
File name	Displays the file name of the telephone logo file.
Buttons	
Load	The specified phone logo file is loaded into the communication system.
Delete	The selected phone logo files are deleted from the communication system.

28.2.2.8 Software Image > Phone Image Logos > Deploy

An image (e.g., a company logo) can be loaded onto the display of the system telephones (OpenStage 40/60/80 or Telekom variants); displayed in the idle state (on-hook). For details on the specification of the logo file, see Telephone Logos .

Parameter Description of Tabs:

- **Deployment of phone logos**

Parameters	Description
Currently Installed Logo Images	
Deploy	If the check box is selected, this phone logo file will be transmitted to the selected system telephones.
File name	Displays the file name of the telephone logo file.
Deploy to Workpoints with Selected Device Type	Selection to determine whether the phone logo is to be sent to all system telephones or only to a specific type of system telephone.

28.2.3 Cordless

Functions for all configured base stations are grouped together under **Cordless**.

28.2.3.1 Cordless > Base Stations

Parameter Description of Tabs:

- **Base station status**

Parameters	Description
Base station data	

Parameters	Description
BS Frequency	The frequencies of the selected base station is displayed here. Up to 10 different frequency channels can be selected simultaneously (see table below).
Base station	Number of the base station.
SW Version	Software version of the base station.
HW version	Hardware version of the base station.
Status	State of the associated port: port active Port not connected Port blocked Port connected, inactive Port connected, inactive 1st expansion port for ... (no. of main port) 2nd. expansion port for ... (no. of main port)
Overload	Number of the overload situations on the UP0/E interface.
Restart	Number of times the base station was restarted.
L1/L2 Error	Number of L1/L2 errors that occurred in the base station.
Abnormal Release	Number of interrupted calls in the base station.
Calls by BS	Number of calls made via the base station (both incoming and outgoing).
Hopping Mode	Cordless Version 2 systems always operate in fast hopping mode, i.e., all frequency - time slot pairs can be used. This provides for 120 duplex channels. In the case of base stations with slow hopping, only every second frequency - time slot pair can be used. This means than only 60 duplex channels are available. All cordless version 1 systems operate in slow hopping mode.
BHO Count OK	Number of successfully completed intracell handovers (bearer handovers BHO), i.e., successful transfer of the carrier frequency and/or the time slot within a radio cell. Not supported by Hicom cordless EM V2.1 and V2.2. Although the meter is not supported, the Bearer Handover feature is available.
BHO Count not OK	Number of intracell handovers that failed (bearer handovers BHO). Not supported by Hicom cordless EM V2.1 and V2.2. Although the meter is not supported, the Bearer Handover feature is available.
Intra SLC Handover	Number of handover procedures within the SLC card. This is counted in the new base station.
Inter SLC handover	Number of handover procedures between SLC cards. This is counted in the new base station.
SLC-wide	
Lost Calls	Number of calls that could not be processed due to a lack of resources.
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.

Parameters	Description
LR Roam	LR Roam counts each connection for a mobile telephone with a default PMID and located at a different SLC. Number of locate request messages that reported roaming (i.e., the current location of the mobile telephone has changed). Each time the mobile phone is switched on, a locate request is executed. If the mobile phone is switched off and switched on again in another radio cell, this meter does not execute a count.
LR Async	LR Async counts each connection for a mobile telephone with a default PMID where the current location SLC is unchanged. This refers to the number of locate request messages which reported layer asynchronicity (i.e., the current location of the mobile phone is unchanged). The count is always performed for the home SLC, and only if a connection is actually set up or supports the CHO with the default PMID. In addition, the criteria for a location update must be met for each connection, i.e., a LOCATE request has been received or the security procedures, authentication (and coding) have been implemented for the link.
HDLC Error	Number of uncritical HDLC error messages that were not reported to the communication system (overflow, underrun, CRC error).
CMI Version	The current cordless version is displayed here.

Frequency (channel)	**DECT**	Europe 1880 – 1900 MHz	Latin America 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 Port/Board Status

The status of all boards can be displayed. In addition, the boards and their ports can be released and locked.

28.2.4.1 Port/Board Status > Board Status

Parameter Description of Tabs:

- **Board Status**

Parameters	Description
Slot	Physical slot number.
Board	Board designation.
Not plugged	Checked if the board is not inserted.
Faulty	Checked if the board is not defective (not charged). It is also possible that a defective or unconfigured board is not displayed.
Is Locked	Checked if at least one port of this board is locked.
Free	Checked if all ports of this board are free.
Res.	Checked if at least one station or line of this board has picked up a call, is being called or is currently being used for an active call.
Clock ref.	Checked if the board provides the reference clock.
Buttons	
Start	Starts the update of the display. The status is updated every 3 seconds.
Stop	Stops the update of the display.

28.2.4.2 Port / Board Status > Out of Service

Parameter Description of Tabs:

- **Port out of Service**
- **Board out of Service**

Parameters	Description
Access	Slot and port at which the station or line is connected.
Call no.	Call number assigned to the port.
Name	Name assigned to the station or line.
Status	Depending on whether or not an allowed station or allowed line is connected to the port, the ports may be **active** or **inactive**. Ports may also be in the **In Service** (default) or **Not in Service through Tool** status, i.e., if they were locked via **Lock card**. The **In Service** status is not identical with **active**. The port status could be **active**, **In Service**, for example, or even **inactive**, **In Service**.
Buttons	
Lock Selection	The selected ports are locked. On locking $U_{P0/E}$ ports, the associated physical port is always taken out of service. Consequently, on selecting a master port, the corresponding slave port is also taken out of service.
Release selection	The selected ports are released.

Parameters	Description
Lock card	The selected boards and their ports are locked. On locking individual mobile phones of a Cordless board, the entire board and thus all mobile phones are always locked. The locking of individual mobile phones is achieved by changing the PIN of the mobile phones.
Release card	The selected boards and their ports are released.

28.2.5 Traces

Trace functions are grouped together under **Traces**. The administrator can start and stop traces and change the trace settings.

28.2.5.1 Traces > Trace Format Configuration

The Trace Format Configuration can be used to define which header data is to be included in the trace output and how the trace data is to be formatted.

Parameter Description of Tabs:

- **Edit Trace Configuration**

Parameters	Description
Data Included in the Trace Header Output	
Global Trace Header Format Settings	When this flag is activated, the options for the following header data can be activated or deactivated. Default value: Enabled
Subsystem ID	When this flag is activated, the subsystem ID is included in the trace output. Default value: Enabled
Task Name	When this flag is activated, the task name is included in the trace output. Default value: Enabled
Task ID	When this flag is activated, the task ID is included in the trace output. Default value: Enabled
Time	When this flag is activated, the specified time is included in the trace output. Default value: Enabled
Module Name	When this flag is activated, the module name is included in the trace output. Default value: Enabled
Line Number	When this flag is activated, the line number is included in the trace output. Default value: Enabled
Formatting of the Trace Data	

Parameters	Description
Full formatting with Parameter Expansion	Standard output mode: All data types are expanded. Trace output: Normal (suitable for normal operation) Default value: Enabled
Limited Formatting (Message types binary, special XTracer format)	In this restricted output mode, the data types are shown in binary format, i.e., as present at the time of the trace. The binary format is intended for analysis with the X-Tracer tool. Trace output: Fast (suitable for medium to high load) Default value: Disabled
Limited Formatting (only basic data types)	In this output mode, only elementary data types (e.g., integer, short, long, string) will be expanded. Trace output: Very fast (suitable for high load) Default value: Disabled
Performance optimized Trace without Parameter Expansion	In this output mode, data type expansion is disabled. Thus, there is also no overhead for trace formatting. Trace output: Extremely fast (suitable for very high load) Default value: Disabled

28.2.5.2 Traces > Trace Output Interfaces

Parameter Description of Tabs:

- **Edit Trace Output Interfaces**

Parameters	Description
File Trace	
Switch File Trace On	When this flag is activated, trace messages in the communication system are written to a log file. Default value: Enabled
Maximum Trace Quota (Kbytes)	Displays the maximum size of the trace memory in kilobytes
Policy to handle reach of max. quota	Option to select what should occur on reaching the maximum trace quota.
Policy to handle reach of max. quota: Wrap Around (remove oldest trace file)	Whenever the maximum trace quota is reached, the oldest respective trace log file is overwritten. Default value: Enabled
Policy to handle reach of max. quota: Stop temporarily the File Trace	On reaching the maximum trace quota, the trace file output is stopped. Default value: Disabled

Parameters	Description
Time between creation of new trace files (sec)	Displays the time in seconds after which a new trace log file is created.
Time range, for which trace files are available	Displays the time range for which trace log files are available.
Trace via LAN (XTracer)	
Switch Trace via LAN On (XTracer)	Trace messages are transmitted via the LAN interface. Default value: Disabled
Timer Value (sec)	Displays the time in seconds after which trace data is transmitted.

28.2.5.3 Traces > Trace Log

Parameter Description of Tabs:

- **Load via HTTP**
- **Clear Trace Log**

INFO: The deletion of trace log data cannot be undone.

Parameters	Description
Trace Log	
Complete Trace Log	All existing trace log files are downloaded
Log from Today	The trace log files of the current day (as of 00:00 hours) are downloaded.
Own Selection	Trace log files of the selected time period are downloaded.

28.2.5.4 Traces > Digital Loopback

They can only be configured using E Manager.

Digital loopbacks are used to test the B channels of S_0, S_{2M} and T1 interfaces of any existing boards. Digital loopbacks should only be activated if requested by the service provider.

Parameter Description of Tabs:

- **Edit Digital Loopback**

28.2.5.5 Traces > Customer Trace Log

This function can be used to start the event display (customer trace). Message types include System, SIP, STUN and LDAP.

Parameter Description of Tabs:

- **Display**
- **Load via HTTP**
- **Clear Trace Log**

Parameters	Description
auto refresh	When this flag is activated, the display for the customer trace log is refreshed automatically. Default value: Enabled
Seconds until next automatic refresh	Time in seconds after which the customer trace log is refreshed automatically.

28.2.5.6 Traces > M5T Trace Components

This function is used to monitor the SIP stack.

Changes to the settings should only be made if requested by the responsible Service Support.

Parameter Description of Tabs:

- **Edit M5T Trace Components**
- **Start/Stop Trace Component**

Parameters	Description
Package Name	Name of the M5T trace component
Trace level	Level of detail for the recording of the MST trace component (trace level 0 = lowest level of detail to trace level 9 = maximum level of detail) Default value: 0
Trace On	When this flag is activated, the MST trace component data is recorded. Default value: Disabled
Crotch	Increment of the activation

28.2.5.7 Traces > Secure Trace

This function is used to record encrypted VoIP payload and signaling data streams.

The recording of encrypted connection data is subject to the mandatory approval of the customer and may only be performed in coordination with the responsible Service Support. For more detailed information on the procedure, see Traces (Secure Trace).

NOTICE: The live recording of calls and connection data is a criminal offence, unless the affected parties have been notified in advance.

Parameter Description of Tabs:

- **Change Secure Trace Passphrase**
- **Import X.509 file for Secure Trace**

Parameters	Description
Change Secure Trace Activation Passphrase	
Current Passphrase	Current password (passphrase) for starting and stopping the secure trace
New Passphrase	New password (passphrase) for starting and stopping the secure trace Value range: 5 to 12 characters
Confirm New Passphrase	Identical new password (passphrase) for starting and stopping the secure trace Value range: 5 to 12 characters
Certificate file (PEM or binary)	Selection of the X.509 file that contains the certificate to be imported into the communication system. After selecting the X.509 file, the fingerprint of the certificate to be imported can be displayed before importing the certificate into the communication system. ***INFO:*** The certificate should be imported only after the fingerprint has been verified.

28.2.5.8 Traces > Secure Trace > Secure Trace Certificate

This function is used to display the imported secure trace certificate.

Parameter Description of Tabs:

- **Show Secure Trace Certificate**

28.2.5.9 Traces > Secure Trace > Secure Trace Settings

This function is used to query the status of a secure trace and to start or stop the secure trace.

Parameter Description of Tabs:

- **Secure Trace State**
- **Start/Stop Secure Trace**

Parameters	Description
Current Secure Trace State	
Secure Trace is active	Status of the Secure Trace
Automatic Deactivation Time	Time at which the secure trace is automatically disabled.

Parameters	Description
Secure Trace for these protocols	Displays the protocols for which the secure trace is created.
Start Parameters	
Secure Trace Activation Passphrase	Password (passphrase) for starting and stopping the secure trace
Duration of Secure Trace (Mins.)	Time period, in minutes, during which the secure trace is to be active. ***INFO:*** Entering a value is mandatory.
Secure Trace for these protocols	
TC (TLS)	When this flag is activated, the secure trace takes into account the TC (TLS) protocol. Default value: Disabled
H.323 Core/HSA (TLS)	When this flag is activated, the secure trace takes into account the H.323 Core/HSA (TLS) protocol. Default value: Disabled
MMX (PEP)	When this flag is activated, the secure trace takes into account the MMX (PEP) protocol. Default value: Disabled
SIP Core/SSA (TLS)	When this flag is activated, the secure trace takes into account the SIP Core/ SSA (TLS) protocol. Default value: Disabled
MSC (SRTP)	When this flag is activated, the secure trace takes into account the MSC (SRTP) protocol. Default value: Disabled

28.2.5.10 Traces > H.323 Stack Trace

This function is used to track problems with components that use the H.323 protocol.

Changes to the settings should only be made if requested by the responsible Service Support.

Parameter Description of Tabs:

- **Edit H.323 Stack Trace Configuration**
- **Edit All H.323 Modules**
- **Load H.323 Trace Log via HTTP**
- **Clear H.323 Trace Log**

Parameters	Description
General	

Parameters	Description
Trace level	Level of detail for the trace (trace level 0 = lowest level of detail to trace level 4 = maximum level of detail) Default value: 2
Console Trace	
Switch Console Trace On	When this flag is activated, H.323 Stack Trace messages are output to the console. Default value: Disabled
File Trace	
Switch File Trace On	When this flag is activated, H.323 Stack Trace messages are written to a log file. Default value: Disabled
Maximum Trace Buffer Size (byte)	Maximum size of the trace buffer in bytes (amount of data stored in the buffer.)
Maximum Trace File Size (byte)	Maximum size of the trace log file in bytes
Trace Timer (sec)	Time, in seconds, after which trace data is written to the log file.
Module Name	Name of the H.323 Stack Trace Module
Trace On	When this flag is activated, the H.323 stack trace module is enabled.

28.2.5.11 Traces > Call Supervision

This function can be used to start and stop the monitoring of trunk and station interfaces (also called subscriber line interfaces).

Parameter Description of Tabs:

- **Start/Stop Protocol**
- **Display**
- **Load via HTTP**

Parameters	Description
Selected Port	Trunk or station interface for which the call supervision is to be started or stopped.
No.	Sequential number.
Time	Time of the event.
Call number / Access	Call number and physical interface.

Parameters	Description
State	State of the interface. The following interface states are possible: • Idle (interface is dormant) • Call Initiated (interface is ready) • Overlap Sending (external sending of digits) • Outgoing Call Proc (end of dialing) • Call Request (waiting for alert) • Call Present (interface is ringing) • Active (interface is in talk state) • Hold (interface is in the hold state) • Disconnect Indication (request to disconnect an active call) • Direct (interface is in speaker call mode) • Intrusion (intrusion is activated.) • Callback A (callback subscriber A) • Callback B (callback subscriber B) • Busy (interface is busy) • Error (error state) • Disconnect PI (waiting for PI (progress indicator) release) • Sensor (signal was sent by sensor.) • Conference Master • Paging • Help Dial (Associated Dialing is used.) • Remote (interface occupied through remote service or DISA) • ACD (call distribution) • Unknown State
Event	Event The following events are possible: • Setup (trunk interface: incoming or outgoing seizure) • Setup Ackn (trunk interface: seizure acknowledgment) • Info (trunk interface: Info (Number Digits)) • Call Proc (trunk interface: unevaluated end-of dialing) • Progress (trunk interface: additional info for call setup) • Alert (trunk interface: evaluated end-of dialing) • Connect (trunk interface: connection of B channel) • Connect Ackn (trunk interface: acknowledgement of connecting B-channel) • Disconnect (trunk interface: request for disconnect) • Release (trunk interface: acknowledgement of disconnect) • Release Compl (trunk interface: connection released) • Monitor On (trunk/station interface: call supervision started) • Monitor Off (trunk/station interface: call supervision stopped) • Off Hook (station interface: handset lifted) • On Hook (station interface: handset cradled) • Digit (station interface: digits are dialed)
auto refresh	If the flag is enabled, the call supervision display is automatically refreshed. Default value: Enabled

Parameters	Description
Seconds until next automatic refresh	Time in seconds after which the call supervision is to be refreshed.

28.2.5.12 Traces > License Component

This function is used to monitor the system-internal license agent (Customer License Agent, CLA).

In a network with a central license, the CLA runs only on the master node. Consequently, slave nodes display the trace settings from the master system.

Changes to the settings should only be made if requested by the responsible Service Support.

Parameter Description of Tabs:

- **Change the CLA trace component**

Parameters	Description
Package Name	Name of the license trace component.
Trace level	Defines the level of detail for the trace of the license trace component Default value: **Standard** (For **OSBiz-S** systems, the default is **All**).
Trace level: Low	Low level of detail for the trace recording.
Trace level: Standard	Medium level of detail for the trace recording.
Trace level: All	High level of detail for the trace recording.
Trace level: Off	License trace component stopped.

28.2.5.13 Traces > Trace Profiles

Trace profiles contain predefined trace components for monitoring complete functional units of the communication system.

Parameter Description of Tabs:

- **Display all Trace Profiles**
- **Add Trace Profile (Empty Profile)**
- **Add Trace Profile (with Current Trace Settings)**
- **Stop all Trace Profiles**
- **Start/Stop Trace Profile**

Parameters	Description
Profile Name	Name of the trace profile
Profile started	Indicates whether a trace profile has been started.
This trace profile is read-only	Indicates whether a trace profile is read-only (all existing default trace profiles are read-only).

Parameters	Description
Trace Component	Name of the trace component
Included	When this flag is activated, the trace component is included in the new trace profile to be added. Default value: Enabled
Level	Level of detail for the recording of the trace component (trace level 0 = lowest level of detail to trace level 9 = maximum level of detail)

28.2.5.14 Traces > Trace Components

Trace components can be used to record the process and status information of individual components of the communication system.

Parameter Description of Tabs:

- **Display All Trace Components**
- **Display Started Trace Components**
- **Display Stopped Trace Components**
- **Edit Trace Components**
- **Stop all Trace Components**
- **Start/Stop Trace Component**
- **Default Trace Settings**

Parameters	Description
Subsystem Name	Name of the trace component
Trace Component Index	Sequential number
Trace level	Level of detail for the trace (trace level 0 = lowest level of detail to trace level 9 = maximum level of detail)
Trace On	When this flag is activated, the trace component data is recorded.

28.2.5.15 Traces > TCP Dump

A TCP dump is used for monitoring and evaluating data traffic in an IP network. An appropriate application is required for the diagnosis of the TCP dump files.

Parameter Description of Tabs:

- **TCP Dump State**

Parameters	Description
Start TCP Dump	Starts the TCP dump
Start Parameter	

Parameters	Description
Interface Name	Interface for which the data traffic is evaluated. The available interfaces are displayed under **Interface Details**. If you select **any**, the data traffic will be evaluated for all available interfaces. Default value: any
Packet Size	Size of data packets to be recorded (in bytes). **0** means that each packet will be recorded in its entirety. Value range: 0 to 2000000000, default value: 0
Criteria for Terminating	
Number of Packets	Number of data packets after which the TCP dump will be stopped.
Time until Stop (sec)	Time in seconds after which the TCP dump will be stopped.
Stop TCP Dump	Stops the TCP dump
Cleanup TCP Dump	Deletes the TCP dump files stored in the communication system
auto refresh	When this flag is activated, the status display is refreshed automatically. Default value: Enabled

28.2.5.16 Traces > rpcap Daemon

An RPCAP (Remote Packet Capture) daemon is used for monitoring and evaluating data traffic in an IP network. The RPCAP daemon enables external applications to remotely access the TCP/IP packets on the LAN interfaces of the communication system. An RPCAP a daemon is often used for long-term traces, since the trace files are stored on a PC and not in the communication system.

NOTICE: The safety notes listed in the tab must be observed.

Parameter Description of Tabs:

- **rpcap**

Parameters	Description
Address to Bind to	
IP Address (either numeric or literal)	IP address of the HOST used for the recordings. Default value: 0.0.0.0
Port (please choose a free one)	Port of HOST used for the recordings.
Trace Internal LAN	When this flag is activated, the data traffic between two boards is recorded via the eth9 interface. Default value: Disabled

Parameters	Description
Client identification to allow access	
IP Address (either numeric or literal)	IP address of the remote client on which the trace is output. Default value: 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.

Parameter Description of Tabs:

- **Kernel Crash Data**

Parameters	Description
Kernel Crash Data service	Status of the service: Green: 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 Traces > Media Server Trace

Media Server Trace can be used to record the process and status information of Media Server component of the communication system.

Parameter Description of Tabs:

- **Edit Media Server Trace Component**

Parameters	Description
Package Name	Name of the trace component Default value: Media Server
Trace Level	Level of detail for the trace (None, Unspecified, Default, Fatal, Error, Warning, Info, Unexpected, Debug, Fine, Finest)
Trace Status	Status of the trace: Green: The trace is enabled. Grey: The trace is disabled.
Start	Starts the Media Server trace.
Stop	Stops the Media Server trace.

28.2.6 Events

The functions for displaying and controlling events are grouped together under **Events**. These include event configuration, for instance, and e-mail settings.

28.2.6.1 Events > Event Configuration

Parameter Description of Tabs:

- **Edit Event Configuration**

Parameters	Description
Event File Settings	
Maximum Event Buffer Size (byte)	Displays the maximum event buffer size in bytes
Maximum Event File Size (byte)	Displays the maximum size of the event log file in bytes
Event Timer (sec)	Displays the time in seconds after which a new event log file is created.
Event via LAN (XTracer)	
Switch Event Logging via LAN On (XTracer)	When this flag is activated, event log messages are transmitted via the LAN interface. Default value: Disabled
Timer Value (sec)	Displays the time in seconds after which event log data is transmitted via the LAN interface.

28.2.6.2 Events > Event Log

This function is used to download or delete the event log file.

Parameter Description of Tabs:

- **Load via HTTP**
- **Clear Event Log**

28.2.6.3 Events > E-mail

Parameter Description of Tabs:

- **Edit E-mail Settings**

Parameters	Description
E-mail Settings	
Subject	Text that appears in the Subject field of the e-mails.
E-mail Address (Recipients)	
Recipient 1	E-mail address to which an e-mail is sent when an event occurs.
Recipient 2	E-mail address to which an e-mail is sent when an event occurs.
Recipient 3	E-mail address to which an e-mail is sent when an event occurs.
Recipient 4	E-mail address to which an e-mail is sent when an event occurs.
Recipient 5	E-mail address to which an e-mail is sent when an event occurs.
Emergency Notifications Recipient	
Emergency Recipient	E-mail address of an on-site security officer to which an e-mail is sent when an emergency number is dialed.

28.2.6.4 Events > Reaction Table

For each possible event, the Reaction Table can be used to independently define what action is to be taken when that event occurs.

Parameter Description of Tabs:

- **Edit All Events**
- **Restore All Events to Default Settings**
- **Edit Event**
- **Start/Stop Associated Trace Profile**

Parameters	Description
Event Name	Name of the event
Send an SNMP Trap	When this flag is activated, an SNMP trap is sent when the event occurs.
Send Email	When this flag is activated, an e-mail is sent to the e-mail recipient specified under **Edit E-mail Settings** when the event occurs.
Associated Trace Profile	Trace profile which is started or stopped when the event occurs.

Parameters	Description
Start Trace Profile	When this flag is activated, the selected trace profile is started when the event occurs.
Stop Trace Profile	When this flag is activated, the selected trace profile is stopped when the event occurs.
Reboot the Gateway	Indicates whether the communication system is restarted when the event occurs.
Reboot the Gateway: Yes	The communication system is restarted when the event occurs.
Reboot the Gateway: No	The communication system is not restarted when the event occurs.
Notify OpenScape	Indicates whether a message is sent to the communication system when the event occurs.
Notify OpenScape: Yes	A message is sent to the communication system when the event occurs.
Notify OpenScape: No	No message is sent to the communication system when the event occurs.

28.2.6.5 Events > Diagnosis Logs

Displays the diagnosis logs (log files) that were created automatically during critical system conditions.

Parameter Description of Tabs:

- **Get Diagnosis Logs**
- **Clearing Diagnosis Logs**

Parameters	Description
File name	Name of the diagnosis log (log file) stored in the communication system
Size (in Byte)	Size of the diagnosis logs in bytes
Modified	Modification date of the diagnosis log
Permissions	Attributes of the diagnosis log: • r = read access • w = write access

28.2.6.6 Events > Alarm Signaling

The stations (system telephones with display, UP0 & HFA) to be notified when the system temperature exceeds 55 degrees Celsius. If the temperature exceeds 60 degrees Celsius, the boards responsible for the overheating (e.g., OCAB, SLAD60/16) are shut down in a controlled manner or switched off.

Parameter Description of Tabs:

- **Edit alarm signaling**

Parameters	Description
Temperature alarm signaling port	
Station 1	Target 1 (subscriber with system phone).
Station 2	Target 2 (subscriber with system phone).
Station 3	Target 3 (subscriber with system phone).

28.2.7 Restart / Reload

Can be used to initiate a restart or reload of OpenScape Business and for a controlled shutdown of OpenScape Business X. In addition, a restart (reboot) of the UC application (UC Smart or UC Suite) or the UC Booster Card (Application Board OCAB) is triggered. To enable the controlled shutdown of OpenScape Business X via a system telephone, a PIN can be defined. In the case of a network, the networked communication systems can be synchronized.

28.2.7.1 Restart / Reload > Restart / Reload

Parameters	Description
System	
Maintain Server	Controlled restart of OpenScape Business: • OpenScape Business S und OpenScape Business X: a controlled restart of the communication system occurs. If OpenScape Business X3/X5/X8 is equipped with a UC Booster Card (Application Board OCAB), a controlled restart (reboot) of the UC Application (UC Smart or UC Suite) also occurs. • OpenScape Business UC Booster Server (Application Server): a controlled restart of the OpenScape Business portion and the UC Application (UC Suite) occurs.
Reload system	Reload OpenScape Business: • OpenScape Business S and OpenScape Business X: the communication system is reloaded. After the subsequent startup, the communication system will be in its default state. All country and customer-specific settings were deleted (system country code = Germany). The communication system has the default IP address 192.168.1.2 and the internal IP range 192.168.3.xxx. The licensing is retained. • OpenScape Business UC Booster Server: the OpenScape Business portion is reloaded. After the subsequent startup, the OpenScape Business portion will be in its default state. All custom (i.e., customer-specific) settings of the OpenScape Business portion (e.g., the User Directory) were deleted. The licensing is retained. The operating system will not be reset.

Parameters	Description
Shut down system	Controlled shutdown of OpenScape Business X: • OpenScape Business X3/X5: The subsequent startup of the communication system is only possible by unplugging and then reinserting the power plug. • OpenScape Business X8: the subsequent startup of the communication system is only possible by switching off all LUNA2 power supplies and then switching them back on again.
Enable/disable shutdown	Define a PIN to activate the shutdown (the controlled shutdown of the communication system) at a system telephone
Restart Application Board	Controlled restart of the Application Board OCAB, including the UC application (UC Smart or UC Suite): During a restart of the Application Board OCAB, all active applications such as myPortal for Desktop and myAttendant, for example, are disconnected. After the startup, all connections are automatically set up again.
Applications	
Sync Network	Synchronization of networked communication systems: After any phone numbers, DID numbers or names have been changed, the data in all networked communication systems are updated through synchronization.
Restart UC Application	Controlled restart of the UC application (UC Smart or UC Suite): During a restart of the UC Application, all active applications such as myPortal for Desktop and myAttendant, for example, are disconnected. After the startup, all connections are automatically set up again.

28.2.8 SNMP

The functions for configuring communities and traps are grouped together under **SNMP**. Communities are used to regulate SNMP data access authorizations. Traps are generated if system problems occur to inform administrators of errors and failures.

28.2.8.1 SNMP > Communities

Parameter Description of Tabs:

- **Display Communities**

Parameters	Description
IP address	IP address of the SNMP communication partner. At address 127.0.0.1, any communication with external IP addresses is blocked.

Parameters	Description
Community	Identification/Access password for the SNMP user. ***INFO:*** To increase security, it is recommended that the default value **public** not be used.
Type	Selection of the type.
Type: Read Community	Communication partner with SNMP read access.
Type: Read Community	Communication partner with SNMP read and write access.
Type: Trap-Community	Communication partner to which error messages (traps) are sent.

28.2.8.2 SNMP > Communities > Read Communities

Parameter Description of Tabs:

- **Display Read Communities**
- **Add Read Community**

Parameters	Description
IP address	IP address of the SNMP communication partner. At address 127.0.0.1, any communication with external IP addresses is blocked.
Community	Identification/Access password for the SNMP user. ***INFO:*** To increase security, it is recommended that the default value **public** not be used.

28.2.8.3 SNMP > Communities > Write Communities

Parameter Description of Tabs:

- **Display Write Communities**
- **Add Write Community**

Parameters	Description
IP address	IP address of the SNMP communication partner. At address 127.0.0.1, any communication with external IP addresses is blocked.
Community	Identification/Access password for the SNMP user. ***INFO:*** To increase security, it is recommended that the default value **public** not be used.

28.2.8.4 SNMP > Communities > Traps Communities

Parameter Description of Tabs:

- **Display Trap Communities**
- **Add Trap Community**

Parameters	Description
IP address	IP address of the SNMP communication partner. At address 127.0.0.1, any communication with external IP addresses is blocked.
Community	Identification/Access password for the SNMP user. ***INFO:*** To increase security, it is recommended that the default value **public** not be used.

28.2.8.5 SNMP > Traps

Parameter Description of Tabs:

- **Display All Traps**
- **Display All Critical Traps**

Parameters	Description
VarBind1 (Severity)	Trap classification: • Critical: error message. This error causes problems. • Major: error message. This error could cause problems. • Minor: error message. The error has no problematic consequences. • Warning: report of a possibly problematic procedure or status. • Cleared: the cause of the error message was resolved (for example, the port is operating again) • Information: plain status messages, no error messages
VarBind2 (Name)	Trap name
Generic Name	General Description such as Enterprise Specific, for example
Specific Name	Type of trap: • 1 = Software • 2 = Hardware
Enterprise	(not used)
Time	Time of error
Index	Sequential number

28.2.9 Admin Log (also called Admin Protocol)

The administrator can use **Admin Log** to change the configuration (e.g., the language) of the administration log.

28.2.9.1 Admin Protocol > Configuration

Parameter Description of the Tab:

- **Edit Configuration**

Parameters	Description
Admin Log Language	Setting of the preferred language for the Admin Log. The Admin Log provides an overview of the changes made at the communication system. Possible languages: German, English, French, Spanish, Italian, Portuguese, Dutch

28.2.9.2 Admin Protocol > Admin Log Data

Parameter Description of the Tab:

- **Load via HTTP**

Parameters	Description
Load via HTTP	Saves the Admin log of the communication system. The Admin log enables you to track when and by whom changes were made to the communication system. All logins at the communication system are logged.

28.2.10 Actions

The functions that support the administrator with repetitive administration tasks such as deleting log data are grouped together under **Actions**.

28.2.10.1 Actions > Manual Actions > Diagnosis Logs

Parameter Description of Tabs:

- **Load data via HTTP**

Parameters	Description
Trace Log	When this flag is activated, the system trace log files are downloaded. The following choices are available: • Complete Trace Log: The full set of existing system trace log files is downloaded. • Log from Today: The system trace log files of the current day (as of 00:00 hours) are downloaded. • Own Selection: From: XXX To: YYY: The system trace log files of the selected time period are downloaded. Default value: Enabled, Complete Trace Log

Parameters	Description
Event Log	When this flag is activated, log files with information about actions and events of the communication system (reset, power on/off, etc.) are downloaded. Default value: Enabled
Admin Log	When this flag is activated, log files with information about administration procedures (login attempts, etc.) are downloaded. Default value: Enabled
Licence Protocols	When this flag is activated, log files with messages about the communication system components that require licenses are downloaded. Default value: Enabled
Customer Trace	When this flag is activated, log files with messages for the customer (remote login, ITSP login, etc.) are downloaded. The messages for the customer trace are provided in a more detailed format than in the trace log, for example. Default value: Enabled
Framework Protocol	When this flag is activated, log files with WBM messages are downloaded. Default value: Enabled
Diagnosis Log	When this flag is activated, the diagnosis logs of the communication system are downloaded. Default value: Enabled
UC Suite Protocols	When this flag is activated, log files with UC Suite messages (UC Suite, SCP and MEB logs) are downloaded. The following choices are available: • Complete Trace Log: All existing UC Suite, CSP and MEB log files are downloaded. • Log from Today: The UC Suite, CSP and MEB log files of the current day (as of 00:00 hours) are downloaded. • Own Selection: From: XXX To: YYY: The UC Suite, CSP and MEB log files of the selected time period are downloaded. All log files are archived together in a compressed file. The following file naming conventions apply to the OpenScape Business logs: UC Suite log files = vs_yyyy_mm_dd.log, CSP log files = csptrace_yyyy_mm_dd.log, MEB log files = mebtrace_yyyy_mm_dd.log Default value: Disabled
Application Protocols	When this flag is activated, log files with messages of the application side of the communication system (for example, CSP protocols) are downloaded. • Complete Trace Log: All existing log files are downloaded • Log from Today: The log files of the current day (as of 00:00 hours) are downloaded. • Own Selection: From: XXX To: YYY: The log files of the selected time period are downloaded. All log files are archived together in a compressed file. Default value: Disabled

Parameters	Description
System Diagnosis Logs	When this flag is activated, the diagnosis logs of the communication system are downloaded. Default value: Enabled
PPP Logs	When this flag is activated, log files with messages for the Point-to-Point Protocol are downloaded. Default value: Enabled
CoreLog Protocol	When this flag is activated, log files with information about the most recent state of the operating system are downloaded. CoreLogs are created during system restart, for example. Default value: Disabled

28.2.10.2 Actions > Manual Actions > DLI Maintenance

Parameter Description of Tabs:

- **DLI Devices Maintenance**

Parameters	Description
Delete Device	Select the system telephone that is to be deleted. With this action, the system telephone is deleted from DLI database. **NOTICE:** Before any DLI Maintenance Action (delete), you must ensure first that the device is not in use anymore.
Call no	Phone number of the system telephone.
Device type	Type of the system telephone.
IP Address	IP address of the system telephone; direct link to the WBM of the system telephone.
MAC Address	MAC address of the system telephone.
Current SW version	Current software version of the system telephone.

28.2.10.3 Actions > Automatic Actions > Garbage Collection

Parameter Description of Tabs:

- **Edit Action**
- **Start/Stop Action**

Parameters	Description
Action Activated	When this flag is activated, automatic garbage collection will be performed on the communication system at regular intervals. After each garbage collection has been completed, the communication system performs a restart (reboot). Default value: Disabled
Start Time (after Midnight)	Garbage collection is performed after midnight. Example: Let us assume that the value entered in the **Hrs** field was 3 and in the **Mins** field was 30. This means the garbage collection action will be started at 3:30 a.m. every morning. Default value: 3 hours, 00 min.
Days on which to perform action	Garbage collection is performed on the selected weekdays. Default value: Enabled

28.2.10.4 Actions > Automatic Actions > DLS Notification

Parameter Description of Tabs:

- **Edit Action**
- **Start/Stop Action**

Parameters	Description
Action Activated	When this flag is activated, the automatic login at an external DLS server is initiated on starting up the communication system. Default value: Disabled
IP address	IP address of the external DLS server Default value: 0.0.0.0
Port	Port of external DLS server Default value: 10444
User name	User name for logging into the external DLS server
Password	Password for logging into the external DLS server

28.2.10.5 Actions > Automatic Actions > SDHC Health Check

Parameter Description of Tabs

- SDHC Health Check

Parameters	Description
SDHC Health Check	
Start Health Check	Enables the immediate Health Check of the card

Parameters	Description
Start Health Check on	Enables a scheduled day, month, year and time for Health Check of the card.
Log File The result of the last fileckecks is displayed.	
Status / Recommended action Recommend actions for every Health Status of the card.	

28.2.11 Platform Diagnostics

Platform Diagnostics Option (only for Development).

28.2.12 Application Diagnostics

Application Diagnostics Option (only for Development).

28.2.12.1 Application Diagnostics > Developer Settings > Trace Console Output

Application Diagnostics Option (only for Development).

28.2.12.2 Application Diagnostics > Developer Settings > Take Over Write Token

Application Diagnostics Option (only for Development).

28.2.12.3 Application Diagnostics > Mainboard

Changes to the settings should only be made if requested by the responsible Service Support.

28.2.12.4 Application Diagnostics> Developer Settings> SIP Provider Profiles

Parameter decsription of tags:

- Add SIP provider profiles
- Edit SIP provider profiles

This page is intended for use by well trained technicians during the certification of a new ITSP. Please read the documents available in the unify wiki: http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#How_to_get_a_new_VoIP_provider_released for more information.

28.2.13 IP Diagnostics

IP Diagnostics Option (Only for Development).

28.2.13.1 IP Diagnostics > Mainboard > Address Resolution Protocol

This function is used to display the data of the Address Resolution Protocol ARP. The mapping table shows the assignment of network addresses to MAC addresses.

Parameter Description of Tabs:

- **Display Address Resolution Protocol**

Parameters	Description
IP address	Displays the network addresses that are currently connected to the mainboard of the communication system.
MAC Address	Displays the physical address of the connected network addresses
Type	Displays the address assignment type. Fixed (static) or dynamic assignment.
Interface	Internal designation of the existing LAN interfaces (e.g., eth0, eth1, eth2, eth3)

28.2.13.2 IP Diagnostics > Mainboard > ICMP Request > Ping

This function can be used to check the network connection between the communication system and a freely selectable target address with a ping command (echo request).

Parameter Description of Tabs:

- **Execute Ping**

Parameters	Description
ICMP Parameter	
Target Address	IP address of the target whose network connection to the communication system is checked using echo request packets. Default value: 127.0.0.1
Number of Echo Requests to Send	Number of echo request packets to be sent for checking the network connection Default value: 3

28.2.13.3 IP Diagnostics > Mainboard > ICMP Request > Traceroute

This function uses ICMP echo requests to determine via which routers data packets are transmitted to the requested target address.

Parameter Description of Tabs:

- **Trace route**

Parameters	Description
ICMP Parameter	
Target Address	IP address of the target whose traceroute to the communication system is checked using ICMP echo requests. Default value: 127.0.0.1
TOS Byte	Indicates whether TOS (Type of Service) bytes are sent. TOS bytes provide information on the quality of a service. Value range: 0 to 255, default value: 0

28.2.14 Online User

Web tool for remote control of OpenStage phones.

28.2.14.1 Online Users

The Online User opens the Java Husim Phone Tester (jHPT). This is a web-based tool to remotely control OpenStage telephones via the Internet. Using a web interface, an existing system telephone is controlled by transmitting real keystrokes and displays of the communication system. Separate documentation is available for the jHPT, which can be downloaded via the Help function of the tool (so no further description of the jHPT pages is provided here).

28.3 Telephony

The functions for configuring the telephony settings (such as subscriber configuration or Call Management (CM), for example) are grouped under **Telephony**.

28.3.1 Basic Settings

Functions for configuring system flags, directory settings and speed dials, DynDNS, Quality of Service, date and time, and call charges are grouped together under **Basic Settings**.

28.3.1.1 Basic Settings > System > System Flags

Parameter Description of Tabs::

- **Edit System Flags**

Parameters	Description
Through-connection for external FWD on	When this flag is activated, calls forwarded to an external destination are put through immediately. The forwarding occurs regardless of whether an internal or external (MSI/ISDN) call is involved. If the call forwarding occurs via an ISDN trunk, and the external forwarding destination is located in another network (such as a GSM network, for example), the call setup from the ISDN Central Office is reported with the progress indicator Leaving ISDN. As of this point in time, the caller incurs connection charges. Default value: Disabled
Call forwarding to main station interface permitted	When this flag is activated, calls over analog trunks (MSI) follow the external call forwarding. Default value: Enabled
Hunting to external call forwarding destination	When this flag is activated, the following applies: if the external call forwarding destination cannot be reached, the call is forwarded to the next destination entered in the call destination list. Default value: Disabled
Conference tone	When this flag is activated, the participants of a conference are reminded that they are currently in a conference call by a special tone at intervals of 20 seconds. Default value: Disabled
Warning signal for call pickup groups	When this flag is activated, a call for a member of a call pickup group is signaled to the other group members with an optical signal (via the display). If the call is not answered within four call cycles (4 x 5 seconds), the other group members also receive a warning tone. Default value: Enabled
Increase volume for optiPoint/OpenStage terminals	When this flag is activated, optiPoint and OpenStage phones are switched to an alternative attenuation plan, which increases the volume. Default value: Disabled
Relocate allowed	When this flag is activated, system telephones can be physically relocated without changing the logical configuration (call number, name, key programming, etc). Default value: Disabled
More than 1 external conference member	When this flag is activated, multiple external subscribers can attend a conference. Default value: Enabled
Trunk reservation, automatic	When this flag is activated, a subscriber can reserve a trunk in advance if there are no free trunks available (busy signal). The subscriber receives a recall as soon as this trunk becomes free and can then set up the external connection. Default value: Disabled
No. redial with a/c code	When this flag is activated, on redialing, any account code that was entered is also repeated in addition to the station number. Default value: Disabled

Parameters	Description
Simplified dialing	When this flag is activated, dialing a single digit at a system telephone immediately triggers line seizure, and the required call number is dialed. It is not necessary to dial the access code. To dial an internal station, one of the following procedures must be used: • Press the Internal key (Mute will change to Internal, if simplified dialing is active) and dial the station number • or press the corresponding DSS key. This function is only available if only one route (see Routes) has been configured. If Entry, ISDN or a/b telephones are still connected in the communication system, LCR with automatic dialing is not possible.
Use only default number for MSN	When this flag is activated, on an S0 bus, MSNs (Multiple Subscriber Numbers) can only be created for already existing internal station numbers (to prevent any possible toll fraud). Default value: Disabled
Path optimization	When this flag is activated, path optimization is performed in networked communication systems. The flag must be enabled for all communication systems belonging to a network. Example for two networked systems (system 1 and system 2): For a call from subscriber A (system 1) to subscriber B (system 2) and subsequent call forwarding to subscriber C (system 1), two trunks are reserved. With path optimization, the connection from A to C is automatically switched over a single trunk. Default value: Enabled
DTMF automatic	When this flag is activated, it causes DTMF mode to be activated each time an outgoing call is set up. This enables answering machines to be checked remotely, for example. Default value: Enabled
Broadcast with connection	When this flag is activated, the Speaker call (Paging) function lets you set up an internal connection without the called subscriber lifting the handset. On lifting the handset, the call becomes a normal two-party call. Default value: Enabled
Tone from CO	When this flag is activated, a connection is switched through to the Central Office or to a networked communication system even if no tone is sent from the peer. Default value: Disabled
Ringback protection	When this flag is activated, collect calls are automatically released. Default value: Disabled

Parameters	Description
Euro-impedance	When this flag is activated, the following impedance values apply in Europe: a/b interfaces for the analog station connection: Input impedance = 270 Ohms + 750 Ohms || 150 nF, Second ringer impedance = 270 Ohms + 750 Ohms || 150 nF, Relative Level A/D = 0 dBr, Relative Level D/A = –7 - 7 dBr a/b interfaces for the analog trunk connection: Input impedance = 270 Ohms + 750 Ohms || 150 nF, Second ringer impedance = 270 Ohms + 750 Ohms || 150 nF, Relative Level A/D = –6 - 6 dBr, Relative Level D/A = –1 - 1 dBr Default value: Disabled
Different phonemail messages Day/Night	When this flag is activated (in a communication system with Voicemail), different Voicemail announcements can be activated for a station by transmitting different station numbers for that station to the Voicemail. As a prerequisite, different call forwarding destinations for day and night modes must be configured for that station. Default value: Disabled
Display international / national code number	When this flag is activated, you can define the display format for system speed dialing (SSD) numbers for incoming calls for which no name is stored in the SSD memory. The complete phone number (PABX number + Direct Inward Dialing (DID) number, including the local area code and country code, if available) is shown on the display of the phone. Example: The SSD number 06671234 was set up without a name. Local area code = 02302, PABX number = 667, DID number = 1234. In the case of an incoming call from 6671234, the number 023026671234 appears on the display. Default value: Disabled
Line change for direct call	This flag is used to define the behavior of a Direct Station Select (DSS) key during an active call on a MULAP trunk. Relevant for Team Configuration / Team Group, Executive/Secretary / Top Group, Basic MULAP, Executive MULAP. On pressing a Direct Station Select (DSS) key, a line change is performed. The call is placed on hold and can only be resumed at this phone. Default value: Disabled (not for U.S. and Canada), Enabled (for U.S. and Canada only)
Automatic redial	Automatic redialing is performed when a called subscriber is busy. The time parameter Timer for automatic redial defines after how much time the redialing is activated. Default value: Disabled
Voice mail Node call number	When this flag is activated for networked communication systems, it defines whether or not the node number must be supplied for the identification of one central or multiple decentralized voicemail server(s). The node number must be supplied for the identification of the voicemail server or servers. Default value: Disabled
Call Pickup after automatic recall	When this flag is activated, recalls and callbacks are also signaled at other members of a call pickup group and can be accepted by them. Default value: Disabled

Parameters	Description
Configurable CLIP	When this flag is activated, instead of the actual station number, the number entered under Clip/Lin is transmitted to the called external connection and presented on the display. If the Clip/Lin entry is empty, the station number is transmitted. Default value: Enabled
Caller list at destination in case of Forward Line	When this flag is activated, in case of a Forward Line Key (MULAP), incoming calls are entered in the caller list of the destination station. Default value: Disabled
Call forwarding after deflect call / single step transfer	When this flag is activated, the following applies: if a subscriber has enabled call forwarding to an internal destination (call deflection), the call is signaled at that destination. After the call forwarding time has expired, the call is signaled at the first destination entered in the call destination list and subsequently at the second destination, if any, and so on. Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C, and the second destination is station D. In this case, the call will be signaled at station C first and then at station D, after the call forwarding time has expired. The activation of this flag only makes sense if the flag Follow call management in case of deflect call / single step transfer is also activated. In order this flag to have any effect the redirecting functions will take place in call, Deflect and single step call transfer, and applies mainly to calls handled via UC (Auto Attendant/ UCD groups) where those redirection functions are applicable. Default value: Enabled
Follow call management in case of deflect call / single step transfer	When this flag is activated, the following applies: if a subscriber has enabled call forwarding to an internal destination (call deflection), the call is first signaled at that destination and subsequently at any further destination entered in the call destination list (after the call forwarding time has expired). Example: For station A, a deflect call to station B was executed. The first destination entered in the call destination list of station B is station C. After the call forwarding time has expired, the call is signaled at station C. In order this flag to have any effect the redirecting functions will take place in call, Deflect and single step call transfer, and applies mainly to calls handled via UC (Auto Attendant/ UCD groups) where those redirection functions are applicable. Default value: Enabled
Warning tone during voice recording	If the flag is enabled, the following applies for OpenScape Business X: If voice recording (Live Call Record) is activated during a call, a corresponding advisory tone is output if the flag is set. Default value: Enabled

Parameters	Description
E.164 numbering scheme	This flag is used to activate or deactivate CDB networking of cross-location or worldwide customer systems. Stations can be reached via a public number (the E.164 call number) in national or international format (for example, internal calling party number in ISDN format), without dialing a node number first. Each station is represented by its E.164 call number, which can be displayed in an optimized format. If the flag is activated, the internal call number is transferred in E.164 format. If this flag is set, SIP stations are registered with the long version of the E.164 call number (location number + internal call number, for example, 4923026673665). Default value: Disabled
Extended Key Functionality	If the flag is enabled, once a key is defined as the "Shift key", only phone numbers without LED support can be saved at the second key level which is now available. Any key functions on the first key level can be programmed. LED signaling is associated with the first key level only. Default value: Disabled
Calling number in pick-up groups / ringing groups / CFN /RNA	When this flag is activated, the station number and name of a caller are displayed at all members of a call pickup group, all members included in a ringing group and at CFN (call forwarding) and CFNA (call forwarding on no answer) destinations. The station number and name are presented on the display. Default value: Enabled
SPE support	When this flag is activated, the Signaling and Payload Encryption (SPE) feature is supported. The VoIP payload and signaling data streams to and from the communication system and between OpenStage system telephones are encrypted. Default value: Disabled **NOTICE:** If you want to use the Cloud Service, Unify Video, then the **SPE Support** must be disabled in order to register the trunk, unless there is a SPE Certificate imported in the System.
SPE advisory tone	When this flag is activated, the following applies: when the system flag SPE Support is enabled, and an OpenStage 15, 20, 20 E or 20 G phone is used, subscribers are notified about an unencrypted connection by a beep tone in addition to the display. Enabling the station parameter Payload Security is a prerequisite for the usage of SPE by a subscriber. No beep tone is heard when using an OpenStage 40, 40 G, 60, 60 G, 80 or 80 G telephone. The status of the connection (encrypted/unencrypted) is permanently shown in the display. Default value: Disabled **NOTICE:** If you want to use the Cloud Service, Unify Video, then the **SPE advisory tone** must be disabled in order to register the trunk, unless there is a SPE Certificate imported in the System.

Parameters	Description
SIP Prov. to SIP Prov. transit	When this flag is activated, transit line connections are allowed for ITSP connections. A connection is a transit connection when a single call occupies two lines in the same communication system. Example: An external is forwarded to an internal station via an ITSP. The internal station then transfers the call again to an external destination via an ITSP. This results in a transit line connection within the communication system. Two trunks are occupied for the duration of the call. The resulting transit line connections are allowed. Default value: Disabled
Transparent dialing of * and # on trunk interfaces	When this flag is activated, Centrex features can be enabled or disabled via IP trunks (ITSP) and ISDN trunks. Several providers offer Centrex (Central Office Exchange) features that can be enabled or disabled by using codes. The input of a code must occur in the dialing state (e.g., after entering the trunk code). The input always begins with * (asterisk) or # (pound). This must be followed by the actual code (digits 0 through 9) and terminated with # (pound). It is not possible to enable or disable Centrex features in the talk state. Centrex features can be enabled or disabled via IP trunks (ITSP) and ISDN trunks. Default value: Disabled
Add seizure code for MEX	Applies only to external calls that are initiated via the ITSP "Mobile Extension (MEX)" feature. If the flag is enabled, the system automatically adds the CO code to the phone number for external outgoing calls if the phone number consists of more than 7 digits, since the system then interprets it as an external phone number. Is the phone number consists of less than 7 digits, the CO code is not added, since the system interprets the number as an internal call number. If the flag is disabled, then the service provider must add the CO code to the phone number for all external outgoing calls. Default value: Disabled
CMI MWI ringer	If this flag is enabled, the Message Waiting Indication (MWI) beep is activated for DECT phones (CMI: Cordless Multicell integration). In other words, when a new message is received in the voicemail box, an alert tone is sent. Default value: Disabled
Automatic Openstage TDM Phones Software Update	If this flag is enabled, when the software version of a TDM phone is older than the software version of the system then the software of the phone is automatically updated. Default value: Enabled

Parameters	Description
Restrict indirect trunk group connections according to CON Matrix	If a company has branches in several cities, then each branch can have a line to the national telecom provider. These branches can also be connected to one another via private tie trunks. For reasons of national regulations (e.g., in India) it can be illegal to make the following connection: A station uses the private tie trunk from their communications system to a private communications system in another city and then a national telecom provider trunk to reach a local external destination. Instead a national telecom provider trunk should be used directly for calls between cities. This requirement is implemented as follows: • Connections between private tie trunks can be restricted by configuring the CON matrix. • For private tie trunks which involve the features Call-forwarding, Transfer and Conference features, the flag "Restrict indirect trunk group connections according to CON Matrix" was introduced. Activating/deactivating this flag has the following effects: – Activated: Calls between cities using private tie trunks are restricted. – Deactivated: Calls between cities using private tie trunks are permitted. Default value: Disabled
Open numbering	
active	When open numbering is used, a station is identified by the node number, followed by the call number or the DID number. This makes it possible to assign the same call number to stations in different nodes. In a networked system, this flag is always set identically for all systems. Default value: Disabled
Node call number	If open numbering is set, the call number of the node must be entered here. A station can be reached from other nodes only by dialing this node call number, followed by the station number. If the total number of digits of the node call number and the station number exceeds 7, a corresponding warning is issued. Default value: Disabled
Transit permission	
Feature Transit	When this flag is activated, transit connections associated with specific features such as external call forwarding, call transfers and DISA applications, for example, are allowed. This applies regardless of whether tie trunk or trunk-to-trunk connections are involved. Default value: Enabled
Tie traffic transit	When this flag is activated, transit connections in direct inward dialing for tie trunk connections (networked communication systems) are allowed. Default value: Enabled
External traffic transit	When this flag is activated, transit connections in direct inward dialing for trunk-to-trunk connections are allowed. Default value: Disabled
Special switch	

Parameters	Description
CALL PROC no send	This flag must be enabled if the service provider should not receive any Call Proceeding Messages (ISDN message) from the communication system. Default value: Disabled
Automatic, cyclical line seizure	If this flag is enabled, outgoing calls will cyclically seize new ISDN trunks when the connection setup fails (e.g., no ACK acknowledgment). Line numbers or route numbers are incremented. Default value: Enabled
Restriction for UC calls	
Restriction for UC calls	When this flag is activated, for all UC calls initiated by the system (e.g., via the Call-Me service), a check is performed before dialing to determine whether the requesting UC user has the requisite class of service for that call. If the UC user does not have the required class of service, the call is not executed. Default value: Disabled

28.3.1.2 Basic Settings > System > Time Parameters

All adjustable time parameters are listed in the table (**Description** column). The timer value for each time parameter can be set via the **Base** and **Factor** columns. The actual time = Base x Factor. If the value 255 is entered in the **Factor** column, this timer is inactive.

Parameter Description of Tabs::

- **Edit Time Parameters**

Parameters	Description
P.O.T. suffix dialing time code / Receiver activation time	Controls the duration of the connection of the code receiver with DTMF terminal units and therefore the ready-to-dial condition. After expiry of this timer the code receiver will be released. Value range: 5 - 15 s
Time for activation of P.O.T features	Will be activated if the signal key is pressed. The signal key helps to distinguish whether a subscriber wants to resume a consultation hold or whether he wants to activate a feature such as conferencing. Value range: 2 - 4 s
Reseizure blocking time	Is started after trunk release and bars an immediate outgoing seizure during this time. Value range: 0 - 5 s
Callback delay time	Is started, if a subscriber changes into idle. Once this time has expired, a check is made to see whether automatic callback is to be implemented. This gives the user an opportunity to make further calls. Value range: 0 - 60 s

Parameters	Description
Length of call back	In case an automatic callback is not answered within this time, the call is finished and the callback is postponed. Value range: 15 - 60 s
Intercept time for automatic recall	If an automatic recall of a blind transfer is not answered within this time, it is intercepted to the attendant console, if this intercept criterion has been configured. Value range: 20 - 600 s
Dial time during transfer before answer	If a blind transfer (to a busy station) is not answered within this time, the recall is forwarded to the extension that transferred the call. Value range: 30 - 600 s
End-of-selection for incomplete dialing (Austria)	Supervisory timer for direct inward dialing. In case no selection occurs during this time, the direct inward dialing is recognized as incomplete or as no dialing. (Austria only) Value range: 10 - 30 s
End-of-selection time (no dialing)	In case selection is not started within a certain time, an end-of-selection is automatically generated. Value range: 5 - 15 s
Time between 1st and 2nd announcement for FAX-DID	Fax/DID, analog direct inward dialing, time after voice announcement. Default value: 15 s
Time for parking + change to hold	Reactivation of a parked call must occur within a timeout. In case the parked call is not answered (resumed) within this time, the station, which has parked the call, will be recalled. With the automatic recall, the hold status reverts to an active status. Value range: 60 - 255 s
End-of-selection for incomplete dialing	In case dialing is not continued within a certain time, an end-of-selection is automatically generated. Value range: 10 - 20 s
P.O.T. Minimum flash time	Defines a minimum time for the recognition of a flash within which the loop must be broken. Default value: 0 s
P.O.T Maximum flash time	Defines a maximum time for the recognition of a flash within which the loop may be broken. Default value: 0 s
Time for activation of automatic recall at attendant console	In case an automatic recall at the attendant console is not answered during this time, the call will be released. Value range: 30 - 180 s
MSI NSA Lead time	Lead time for the rotary dial normally open contact (NSA); is used to prevent dialing noise in the handset for pulse dialing equipment (before the pulse). Default value: 0 s

Parameters	Description
MSI NSA Follow time	Follow time for the rotary dial normally open contact (NSA); is used to prevent dialing noise in the handset for pulse dialing equipment (after the pulse). Default value: 0 s
Fault extraction time for ring	Time to hide line faults for pulse dialing. Default value: 0 s
End-of-dialing for 1A dialing	Indicates the time after which the last digit will be dialed out for the 1A procedure. The outdialing of a digit occurs after input of the next digit. The last digit is dialed after expiry of the timer or if it is marked with the end of dialing indication (#) by the station. Value range: 4 - 4.5 s
Additional charge time	When a trunk is released, incoming call charge information (call charge pulses) on analog trunks can be analyzed by the communication system during this time. The trunk is blocked for outgoing connections during this time. Default value: 0 s
Interdigit time for pulse dialing	Allowed delay between each digit for pulse dialing Default value: 10 s
Dial tone monitoring time	This is the waiting time for dialing tone. In case this timer expires, the system assumes a failure of the trunk. The trunk will be marked as "failed". Default value: 10 s
Pause duration for pulse dialing	Pulse dialing occurs through pulse-pause sequences and the detection of pauses on pulse-dialing lines. Default value: 0 s
Pulse time for pulse dialing	Pulse dialing occurs through pulse-pause sequences. Detection of pulses on pulse dialing lines. Default value: 0 s
Flash time for PBXs	Break time for station loop to trigger control functions (e.g., consultation) in the system. Default value: 0 s
Flash time for trunks	Break time for station loop to trigger control functions (e.g., consultation) on the MSI line. Default value: 0 s
Minimum pulse time for pulse dialing-P.O.T.	Pulse dialing occurs through pulse-pause sequences. Detection of pulses from the pulse dialing phone. Default value: 0 s
Maximum pulse time for pulse dialing-P.O.T.	Pulse dialing occurs through pulse-pause sequences. Detection of pulses from the pulse dialing phone. Default value: 80 ms

Parameters	Description
Transmission time for DTMF signals	Country-specific duration of DTMF dial characters. Default value: 80 ms
Pause between DTMF signals	Country-specific pause between DTMF dial characters. Default value: 80 ms
MOH delay timer	In case a connection is held, music on hold is applied, if configured. However, MOH is only activated after this time has expired, in order to make sure that activation of features such as conferencing is not hindered by MOH. Value range: 1 - 5 s
Pause before dial (only for Development)	If dial tone detection is not possible or desired for analog trunks, dialing can be automatically initiated after this time period. Default value: 3 s
Minimum charge pause	Time between call charge pulses. Default value: 0 min.
Minimum charge impulse	Duration of call charge pulses. Default value: 0 min.
NSA Answer pulse time	Rotary dial normally open contact (MSI lines) Default value: 0 s
NSA Seizure pulse time	Rotary dial normally open contact (MSI lines) Default value: 0 s
Release if no dialing	In case of a trunk seizure and no dialing within a certain time, the connection is released. The subscriber will get busy tone. Value range: 5 - 30 s
DP P.O.T. Minimum interdigit time	Time between dialed digits for pulse dialing telephones. Default value: 0 ms
DTMF P.O.T. flash debounce time	Prevents multiple detection of Flash button. Default value: 0 ms
DTMF Settling time	Waiting time to avoid disruption of DTMF signals on outgoing lines. Default value 100 ms
Flash settling time (see help)	Waiting time after flash on analog lines. Default value: 1 s
Cycle length for recovery	Time for restart of analog lines, after no dial tone was detected. Default value: 120 s
Dial pause length	Indicates the length of the pause to be implemented between two digits, if a pause mark is detected. Value range: 1 - 5 s

Parameters	Description
Fault extraction time for calls in PABX operation (see help)	Time to hide line faults. Default value: 0 s
Artificial end-of-selection	With external dialing, received digits after artificial end-of-selection are interpreted as consultation hold. Value range: 5 - 15 s
Timer for automatic redial	If the station is busy, the relevant number is automatically redialed when the timer elapses. This feature does not work unless the option Automatic redial is selected under Flags. Value range: 10 - 650 s
Fault extraction time for the first polarity change (France/Spain)(see help)	Time to hide line faults. Default value: 0 ms
Delay for announcement prior to answer	Adjusts the delay time, after which the announcement device answers. Value range: 1.5 - 30 s
Time between HAT analysis and dialing of trunk main station interface	Determines the time between the audible tone recognition and the dialing of the first digit via analog trunks. Value range: 0 - 2 s
Pause length after dialing 2nd discrim. digit	Determines the length of the pause to be implemented after dialing the 2nd route seizure code or the international code number. Transfer to the next switching node Value range: 1 - 5 s
Time until warning tone in main station interface transit connection	Transit connections are monitored depending on the type of protocols. This is to avoid, that a connection remains endlessly. If at least one trunk in this transit connection has release recognition, the time is not monitored (see the exceptions in the table below). There is no release recognition for analog trunks. However, there is a hardware option for silent reversal. This makes release recognition possible for analog trunks. The Table for transit monitoring (the following is valid for the trunk types specific to the US:) shows the trunk types where a monitoring timer is implemented. The length of the monitoring can be configured. However, when using an analog trunk with silent reversal, note that there are call numbers where it's possible that there is no answer and therefore where no release can be recognized. As a rule, these call numbers are for announcement services. This must be explicitly pointed out to the operator of the communication system. Value range: 120 s - 42 min
Time from warning tone until release...	In the case of monitoring the time for transit connections, a warning tone occurs after the monitoring timer expires. So that the call can be ended, the connection is only cleared down after this timer has expired, and not immediately. Value range: 10 - 650

Parameters	Description
Release time for MSI	A call to an MSI line via direct inward dialing (DID) is released after this time if no call was connected. Value range: 30 s - 254 min
After holding, a warning tone is switched (Italy)	After expiry of this time, camp-on occurs with the held connection at the subscriber who held the call (ITL). Value range: 30 - 180 s
LCR: Artificial end-of-selection	Waiting time after the last digit until end of dialing is assumed (block dialing LCR). Default value: 5 s
Monitoring a UCD call to an analog line	Time for activation of an MSI call to a UCD group when no connection has been set up. Value range: 10 - 3810 s
Monitoring transfer to a UCD group prior to answer (only for Development)	If a transfer to a UCD group occurs prior to an answer, the timer is started. If the transferred call is not answered, an automatic recall occurs following the timeout. Value range: 10 - 3810 s
Delay timer for attendant console	Time until update message is sent to the PC Attendant Console (Business Attendant). Value range: 300 ms
USBS timer interval	For access via S0 port, TA-S0, TA-RS232 and TA-API the User Signaling Bearer Service (USBS) based on ETS 300 716 is used. Value range: 1 - 60 s
Timer for Toll Fraud Monitoring	When this timer expires, an active transit connection is signaled at the display of the attendant console. The attendant will be able to release the transit call. This enables the monitoring of transit traffic. Value range: 0 - 650 s
Special busy tone, if destination doesn't answer the call	After expiry of this timer, the calling subscriber gets the special busy tone. Value range: 30 - 120 s
Special busy tone, if trunk is seized without dialing	In case a subscriber seizes an outgoing trunk without dialing, he will get a special busy tone after expiry of the timer. Value range: 20 - 60 s
Calling time transfer before answer on busy station	After expiry of this timer, subscriber A, which has been transferred from subscriber B to a busy subscriber C, is transferred back to subscriber B. Value range: 15 - 180 s

Parameters	Description
Error signaling interval	The error signaling time defines an interval in the value range 1 to 15 minutes. Decimal places are rounded up to full minutes, values under 1 min. or above 15 min. are evaluated as 15 min. The current Class B error entered in the event log is transferred cyclically to the remote center when the interval has elapsed. Value range: 60 - 900 s

28.3.1.3 Basic Settings > System > Display

Parameter Description of Tabs:

- **Edit Display**

Parameters	Description
Display name / call number	It is possible to configure which of the following data is displayed for calls on the screens of all connected telephones: Calling ID only, Name (if present), or both Name and calling ID at the same time. If a telephone does not support one of these settings, instead of displaying the name and the calling ID at the same time, only the calling ID may be shown, for example. OpenStage telephones support the simultaneous display of the name and calling ID. Default value: Name and calling ID
Display name / algorithm	Full name support is done with three fields, one for the first name, one for the last name and a third for the display name. Display name field can store up to 16 characters, name and last name fields can store up to 32 characters. One of the following options of the display name algorithm can be used: • <last name>, <first name> • <last name>, <first name initial> • <first name>, <last name> • <first name initial>, <last name> • <last name> Default value: <last name>, <first name>
Transfer before answer	If a call is transferred before it has been answered, either the number of the party transferring the call or the number of the party placing the call can be displayed at the receiving station. A call which was switched by "Transfer before answer" cannot be rejected by the called party. If Transferred by is selected, the display will show the transferring party before the connection is established and after the call is released. If Transferred to is selected, the display will show the transferring party as long as the transferring party is connected to the receiving station. After the transferring party releases the call and there is a connection, the display will change from the transferring party to the transferred party. Default value: Transferred to

Parameters	Description
Automatic recall	If a call is transferred and then recalled, either the number of the party transferring the call or the number of the party recalling the call can be displayed at the receiving station. An internal B station displays the call transfer. C receives a ring tone until either B answers or A recalls. This item can be used to configure what is to be shown on the display of transfer destination B: either station A (caller) or C (transferred destination). If an automatic recall is started from station A, both stations receive the display no reply. Default value: Transferred destination
Date/Time format	The date can be displayed in various formats. Default value: Europe - 24 hour format
Caller list, mode	If Internal and external calls or Only external calls is activated, all calls that were not accepted are saved in a list whose contents can then later be retrieved using a system procedure. If All external calls whether answered or not is activated, then calls that have been accepted are also saved in the caller list. No call numbers are removed from the caller list, either for incoming or outgoing calls. If all of the memory locations in the caller list have already been used, the oldest entry is overwritten when an additional call number is saved. Calls that have not been accepted are displayed in the manner already described in the Missed Calls List feature. Calls that have been accepted are displayed in the same manner as for the "Save call number" functionality of the caller list. If an external incoming call is routed via the AutoAttendant to an internal station and the station is currently busy or has call forwarding activated, no entry is made to the missed calls list. Default value: External calls only
Call number suppression	When this flag is activated, the calling number is not displayed in ISDN, i.e., the called party does not see the calling number (this feature also needs to be activated at the telephone company). There are call scenarios in which a caller may have been set to "presentation restricted" by the Central Office. If this flag is enabled, the caller's number is displayed to the called party. If this flag is disabled, the text "Number unknown" appears. The flag always depends on the CO settings of each provider. Default value: disabled
Internal Phonebook	Users can access a system-wide online directory (phone book) that includes names and call numbers for all internal extensions. System-specific display terminals allow users to scroll through the directory, to display all available internal stations with their names and call numbers, and then dial any of the stored numbers. Terminal devices with alphanumeric keypads can use this to search for a specific number. Select the appropriate option from the list: no: No access to the directory is possible; internal: Access to the internal directory (stations, groups and speed-dial destinations) is possible; LDAP: Access to the directory information of the LDAP server. LDAP access must be configured via LDAP for this purpose; all: Users can choose between accessing the internal directory or the LDAP directory. Default value: Internal

Parameters	Description
Internal Phonebook via Unified Directory	When this flag is activated, the user can search contacts in all directories. The search/lookup requests are handled as requests to the Unified directory. When the flag is not activated, the search/lookup requests are handled locally from the system. Default value: Enabled
Switches	
Call timer display	No call charge information is displayed for outgoing external calls. For UP0/E devices with a display, the current call duration is displayed. For analog lines, time recording is started by a timer (five seconds after the end-of-dialing) and for digital trunks with CONNECT. The communication system does not support call duration display for S0 devices. Default value: disabled
DTMF closed display	When PIN codes are entered on system telephones with a display, only asterisks (*) are shown on the display. Default value: enabled
Display for info message	Info messages are shown on the display of system telephones. Default value: enabled
Outreach call number transparent	If a call is forwarded to an external station, the number of the calling station is displayed at the called station. In a networked system, the option must be set in the node at which a trunk connection is activated. This feature is contingent on the explicit release of the chargeable function Clip No Screening in the CO. This flag works as a toggle with the flag Suppress station number under Routes. Default value: disabled
SST with transfer option (transfer caller's number)	With the flag activated, when the user selects the "Start Transfer?" menu option (while on an active call) the transfer will be executed as Single Step Transfer (no consultation call). If the user selects to make first a consultation call (e.g. "Enquiry?" option) and then transfer the new call to the held party, then the transfer will be executed as normal blind transfer (or transfer after answer). In case of Single Step Transfer the calling number is displayed at the external destination when the mobile device rings, i.e. the called party sees the calling number and not the number of the transferring party when the call is transferred by a system device. The flag "Outreach call number transparent" must be also activated. Default value: disabled **NOTICE:** If the transferred party is an external device, then the function CLIP no screening must be supported by the Network Provider and activated. Otherwise, the default DID of the system will be used from CO, or the call will be rejected from CO.

28.3.1.4 Basic Settings > System > DISA

Parameter Description of Tabs::

- **Edit DISA**

Parameters	Description
DISA	
Direct inward dialing	Phone number under which the DISA function can be reached from external locations. The call number may be different for external and internal use.
Security mode	In order to be able to use the DISA functions, the user must enter a password. With the Security mode options, one can establish whether the user must wait after entering the password or whether he/she must enter the pound symbol (#). Default value: After Timeout
DISA internal	
Phone number	DISA internal refers to usage at some other IP-networked node.
Mobility Callback	
Direct inward dialing	The authentication via password is not required if a call recognized as a mobility number is made externally to a Mobility Callback DID number. In this case, the internal dial tone is switched on directly. This requires the device of the external subscriber to transmit its phone number. This phone number is then checked against the Mobility list.

28.3.1.5 Basic Settings > System > Intercept/Attendant/Hotline

Parameter Description of Tabs:

- **Edit Intercept/Attendant/Hotline**

Parameters	Description
Intercept Position	
Day/night	Call number of intercept position. The intercept position can be defined separately for Day and Night. In addition, it is also possible to enter any destination when activating the night service (variable night service).
Central intercept position	
Route	Route index for the central intercept position in networked communication systems
Call number	Call number of the central intercept position in networked communication systems
Intercept to intercept position	

Parameters	Description
On RNA	The call follows the defined procedure for incoming calls. If the end of the table is reached and does not answer, the system checks to see whether or not intercept after timeout applies. In this case, the intercept position is called after the number of rings specified under Call Forwarding. Intercepts cannot extend beyond a hunt group. The call is forwarded to the first hunt group station and remains permanently in the hunt group. Default value: enabled
on Busy	If a line is busy, the system first checks to see whether or not a waiting call can be signaled. If it is not possible to signal a waiting call (call waiting rejection or intercept criterion), then the call follows the Call Management/Call Routing procedure. If the call cannot be signaled at any station, the system checks to see whether intercept or clear-down applies (B signal to CO). If an analog telephone with call waiting rejection is busy, the call is cleared down, regardless of trunk type. In the case of DTMF direct inward dial and MSI, the call is always intercepted. Default value: disabled
On Invalid	When a wrong number is dialed, the system checks to see whether intercept applies. In the case of DTMF direct dial, the call is always intercepted. Default value: enabled
On Incomplete	If the dialed station number is incomplete, the intercept position is called after the preset time has elapsed. The time can be set under the Time Parameters in the "End-of-selection for incomplete dialing" field. Default value: enabled
On unanswered recall	If an external call is not picked up by the B subscriber after the A subscriber implements Transfer before answering to the B subscriber, and the call is still not picked up after a recall to the A subscriber is implemented, the intercept position is called after a defined period. The time can be set under the Time Parameters in the "End-of-selection for incomplete dialing" field. If this flag is not activated, the call is cleared down after the defined period. Default value: disabled
On rejection	If an internal subscriber rejects a call with "Reject incoming call", the call follows the call management / call routing. If the call cannot be signaled at any station, the system checks to see whether intercept or clear-down applies (B signal to CO). Default value: enabled
Telephone lock intercept	
Call number	If the telephone lock for a station is active and a trunk group code is dialed from that station, the call is immediately forwarded to the intercept destination entered here. This means that if a user dials a number that is not authorized, the call will be signaled on the station number assigned here. The Codelock intercept function is set individually for each station via station flags.
Switched Trunk Authorization	
Switched Trunk Authorization	In this field, you must configure a station with unrestricted trunk access, otherwise Deflect Call to an external destination will not be possible.

Parameters	Description
Attendant code	
Internal call number	This is the call number used by internal devices to reach the Intercept position. Value range: Free input of any digit, provided it is not already used in the dial plan.
Call Number External	This is the call number used by DID calls or calls from the network (CorNet-N or CorNet-NQ) to reach the Intercept position.
Hotline	
Off-hook alarm time	If a subscriber lifts the receiver, the hotline is automatically called once the off-hook alarm time has expired. However, this only happens if the subscriber does not enter any digits during this time. The off-hook alarm time is specified in seconds.
Destination call number 1-6	Six hotline destinations can be entered system-wide; the selection occurs per station (see Stations / Edit station parameters)
Attendant Console	
Queued calls	In the Queued Calls field, you define the maximum number of calls that can wait in the Attendant queue. If the number of stations waiting in the queue of the attendant reaches this numerical value, the calls are forwarded to a configurable overflow destination. Value range: 1-15
Wait time	Here you enter the number of seconds that a call can wait in the queue. After this time has expired, the call is are routed according to the call forwarding defined via the Call Management.
Speed extending	If this flag is set, the attendant can transfer the call to another party by entering the station number for that party. This speed call transfer can only be used when the system-wide flag **DTMF automatic** has been disabled. Default value: disabled
Extend Undialed Lines	An authorized subscriber (attendant console AC) can transfer an undialed trunk to an internal subscriber who does not have sufficient direct trunk access so that this subscriber can conduct exactly one external call. After the trunk is transferred to the subscriber without sufficient direct trunk access, toll restriction takes place based on an additional direct trunk access for transferred trunks. The outgoing external call is allowed only if this additional direct trunk access is sufficient, for example, if the subscriber dials a valid number according to the denied or allowed list for transferred trunks. The subscriber must dial the seizure code on a transferred trunk. A CO call privilege can be configured in the communication system for each trunk group via a reference subscriber. The default reference subscriber is the first logical subscriber port or the attendant console. The default setting is set to unrestricted trunk access for all trunk groups. Default value: disabled
Other criteria	

Parameters	Description
Call waiting on Busy	If this flag is activated, the "Call Waiting" feature is enabled for all stations in the communication system. Default value: enabled
Immediately camp on for attendant calls	Only relevant in CorNet networked systems. If the flag is set, call waiting is only allowed when an attendant console (system A) calls station B (system B). All other stations of system A cannot reach system B via call waiting. For the stations in System B, the condition for call waiting rejection (see Station view: Flags) applies to the respective stations. If the flag is not set, all calls to busy stations in another system are switched through via call waiting, provided the station has not turned on the call waiting rejection option. This flag must be set if you want to place the calling intercept on hold immediately and enable call waiting when a station is busy. If this flag is not set, the intercept receives the busy signal and is only placed on hold after a few seconds. Default value: disabled
Override by AC	If this flag is enabled, the intercept position is authorized for the "Override" feature. This enables the Attendant to override (i.e., intrude into) a call of an internal subscriber. Default value: enabled

28.3.1.6 Basic Settings > System > LDAP

Parameter Description of Tabs:

- **Edit LDAP**

Parameters	Description
LDAP access	
IP address of the LDAP server	IP address of the LDAP server from which the directory information is to be retrieved.
Port number for LDAP access	Port number for LDAP access. Default value: 389
User name/password	Under Windows Server ADS, anonymous access is not supported. In this case, enter your user name and password for the LDAP connection here. Value range: max. 48 characters
LDAP server parameters	
Basic DN	DN = Distinguished Name, search base for the search query to the LDAP server (ASCII, 100 characters), e.g., ou=com, cn=unify, cn=de

Parameters	Description
Search query	Pattern for the search query to the LDAP server. The $ character must be entered as a placeholder for the names to be found. Note that a search pattern cannot start with a regular expression. Value range: ASCII, 50 characters Default value: cn=$*
Result attribute, Name	The result attribute name supports characters from the ISO-8859-1 character set with code values in the range from 0x20 to 0x80 (ASCII characters), as well as the characters Æ, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. The display of characters depends on the language setting of the station and the phone being used. Value range: ASCII, 24 characters Default value: cn
Result attribute, Station number	Up to 25 dialed digits (0...9, *, #) and 6 characters for formatting (+,(), spaces, -) may be returned in the result attribute Station Number. The station number must be in the canonical call number format (e.g., +49 (89) 70070) Value range: ASCII, 25 characters Default value: telephoneNumber
Sort search results	The search results are sorted alphabetically by name. Default value: enabled
LDAP Call Number Evaluation	
LDAP seizure code	The seizure code matches the dialed routing code. Default value: 0 (default routing code of the first route)
LDAP station number prefix	The prefix specified here is placed before the found call number. Value range: ASCII, 5 characters

NOTICE: For the LDAP resources to be displayed you have to select the appropriate option under **Basic Settings** > **Display** > **Internal Phonebook** in the **Display** menu. For more information see chapter 28.3.1.3 Basic Settings > System > Display.

28.3.1.7 Basic Settings > System > Texts

Parameter Description of Tabs::

- **Edit System Texts**

Parameters	Description
Reset to default values	Resets the messages and answer texts to the predefined values for a given language. A reset occurs by selecting a language from the drop-down list.

Parameters	Description
Info texts	Information texts are short messages that one station can send to another. The communication system supplies ten standard Info texts. Each of these standard texts can be overwritten. There are only ten possible messages available at any time. Users access this information texts via the Send Message? menu item on their system telephones. Stations with which have an alphanumeric keypad also have the option of creating their own messages; however, they can not change these default messages. Value range: max. 24 alphanumeric characters
Answer texts	Short messages that are sent to callers when users are absent. Ten standard texts are available. Each of these standard texts can be overwritten. Stations with which have an alphanumeric keypad also have the option of creating their own messages; however, they can not change these default messages. For many situations, users will only need to add individual information to the existing messages. Texts with a colon give the station the opportunity to complete the message by adding a number or a date. Users access these answer texts via the Advisory Message On? menu item on their system telephones. Value range: max. 24 alphanumeric characters

28.3.1.8 Basic Settings > System > Flexible Menus

Flexible menus allow you to customize the menu items shown in the service menu of system telephones. If the check box is selected in the **Masking list**, the menu item is not displayed. This setting applies system-wide to all system telephones. Hidden functions can still be activated with a code.

28.3.1.9 Basic Settings > System > Speed Dials

Up to 8000 directory entries can be manually created or modified. The speed dial destinations are central system speed dial numbers (SPDC). The entries in a column can be sorted by clicking on the corresponding column name.

Parameter Description of Tabs:

- **Change Speed Dial**

Parameters	Description
Speed dial	Number that is selected by the subscriber. Speed dial numbers must have four digits (`0000–7999`; use leading zeros).
Phone number	Dialable call number of the desired destination, i.e., a seizure code or trunk code (e.g., 0, 9, 81 or 801). Value range: max. 31 digits

Parameters	Description
Name	Name for the speed dial destination, as stored in the internal directory and displayed when dialing the corresponding speed dial destination. Incoming calls (with CLIP are compared to the stored speed-dialing destinations and displayed as the name of the speed-dialing destination, as long as the display parameter name or the name and calling ID is activated. Value range: max. 16 characters
Search	Entering a search term in the **Speed dial**, **Call number** or **Name** search fields and then pressing the return key causes all hits containing the specified search term to be displayed. For example, entering the call number `521` would display the matches `+495213535` and `+498967521`, and entering the term `co` as the name would display `Collins`, `Mcoin` and `Branco`. Pressing the return key with nothing entered in any of the search fields causes all entries to be displayed.
Buttons	
Apply	Add new entries or edit existing entries.
Undo	Undo changes to existing entries (before Apply).

Parameter Description of Tabs:

- **Import/Export CSV/XML file via HTTP**

Parameters	Description
Import CSV/XML file via HTTP	Speed dial destinations can be imported via an XML file in UTF-8 format. Existing speed dial numbers are deleted before the import. An XML template for importing speed-dial numbers can be found under **Service Center** > **Documents** > **CSV Templates.**
Export XML file via HTTP	Speed dial destinations can be exported as an XML file in UTF-8 format. The export always includes all the records. **NOTICE:** Import of speed-dial lists from CSV files is not recommended any more and it's only supported for old customers.

28.3.1.10 Basic Settings > System > Service Codes

Features can be enabled or disabled via the phone by using service codes. The standard service codes can be changed, provided the assignment of the codes is consistent.

In addition the two codes used on Dial Pulse telephones and ISDN devices to replace the * (star, default: `75`) and the # (pound, default: `76`) keys can also be changed (substitutions).

28.3.1.11 Basic Settings > System > HFA Registration Password

Parameter Description of Tabs:

- **HFA Registration Password**

Parameters	Description
The following prerequisites must be satisfied for this parameter to be effective: the system telephones must use the DLI of the system, and the DLI must be able to supply the system telephones with the required parameters.	
Change HFA Registration Password The HFA registration password can be changed by the administrator	
Enforce authentication for HFA devices	The following options in the drop-down list are available: • **No** (default value) - no authentication is applied If this option is selected, the password fields are disabled. By clicking on the **Apply** button, the authentication is disabled. • **Only non Deskshare devices with DLI** - the password will be applied only to the System clients that have DLI configured. The password will be set in system DB for those devices and will be distributed to the proper ones by DLI. • **Only Deskshare devices with DLI** - the password will be applied only to the deskshare devices that have DLI configured. The password will be set in system DB for those devices and will be distributed to the proper ones by DLI. • **All non Deskshare devices** - the password will be applied to all System clients. The password will be set in system DB for all those devices and will be distributed to the proper ones by DLI. For the System clients that do not have DLI configured, the password must be entered manually to each of them in order to come into service. • **All Deskshare devices** - the password is applied for all enabled devices. The password will be set in system DB for all those devices and will be distributed to the proper ones by DLI. For the deskshare devices that do not have DLI configured, the password must be entered manually to each of them in order to come into service.
Password	The password must be entered in this field. The length of the password must be at least 8 characters with at least 1 digit and/or 1 letter.
Confirm Password	The password must be repeated in this field for verification purposes.

28.3.1.12 Basic Settings > Gateway

Parameter Description of Tabs::

- **Edit Gateway Properties**

Parameters	Description
General	
Customer name	Freely definable name for the customer; only for informational purposes (optional) Value range: max. 15 characters
Contract number	Freely definable string for informational purposes only (optional) Value range: unlimited
System name	Freely definable name for the communication system. This string appears on the display of all system telephones. Value range: max. 24 characters
Gateway Location	Freely definable string to specify the physical location of the communication system. This information helps a service technician to find the communication system when physical access to the communication system is required. (optional) Value range: unlimited
Contact Address	Freely definable string to specify the person to be contacted if problems arise with the communication system. (optional) Value range: unlimited
System Country Code	Selection of the country in which the communication system is operated; changing the system country code requires a reboot, which is carried out automatically.
Gateway IP address	Displays the IP address of the communication system, e.g., 192.168.1.2.
Gateway Subnet Mask	Displays the subnet mask of the communication system, e.g., 255.255.255.0.
International Prefix	Entry of the prefix for international calls, e.g., 00 in Germany or 011 in the U.S.
National Prefix	Entry of the prefix for national calls, e.g., 0.
Brand	Selection of the purchased product (OpenScape Business or Octopus or FX)
Gateway Location	
Country code	Enter the country code prefix, e.g., 49 for Germany or 1 for the U.S.
Local area code	Enter the local area code (e.g., 89 for Munich)
PABX number	Specifies the PABX number (central number without station DID), e.g., 7007
Network Parameters	
Node ID	Each node in a networked system must be assigned a unique node ID. This enables the individual nodes in a networked system to be uniquely identified. Value range: 1 to 100
Internal dial tone	

Parameters	Description
Continuous tone	If this flag is set, the internal dial tone is not a tone sequence, but a continuous tone. The internal dial tone is heard immediately on picking up the handset and before any digit has been dialed. Default: disabled

28.3.1.13 Basic Settings > DynDNS > DynDNS Service

Parameter Description of Tabs::

- **Display DynDNS Configuration**
- **Edit DynDNS Configuration**

Parameters	Description
Activate DynDNS	The DynDNS service can be used to access the gateway from different locations without knowing the current IP address of the gateway. The DynDNS service can be enabled here.
User-defined Domain	Select this check box if you cannot find the DynDNS provider in the **Domain name** list.
User name	User name of the DynDNS account at a DynDNS provider. A new DynDNS account can be created at the Internet address `http://www.dyndns.org/account/create.html`, for example.
Password	Password of the DynDNS account at a DynDNS provider. For security reasons, only wildcards are displayed when typing the password in this field.
Retype Password	Repeat password of the user account with the DynDNS Service. For security reasons, only wildcards are displayed when typing the password in this field.
Hostname	Entry of the host name registered with the DynDNS provider without the domain name, e.g., myhost. The complete subdomain name is composed of the host name and the domain name, e.g., myhost.dyndns.org.
Domain name	Selection of the DynDNS provider from a list (e.g., dyndns.org) or through manual entry of the DynDNS provider (if **User defined Domain** has been enabled).

Parameters	Description

Update URL	Here you can enter the update URL of a provider which does not appear on the list of DynDNS providers. The syntax of this URL depends on the DynDNS provider. In addition, customer-specific parameters (shown in *italics* in the example) must be supplemented.
	Example of an update URL:
	`http://www.anydns.info/update.php?user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>`
	Example of an update URL with base64-encoded authentication:
	`https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update?hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> for Base64-encoded parameters

Last Update	Time when the DynDNS service was updated last.
IP Address at DynDNS	IP address at the DynDNS provider to which requests for your configured DynDNS subdomain are routed.
Own dynamic IP Address	Displays the current IP address of the communication system, which was assigned by the Internet Service Provider.
Enable Wildcard	If you enable this option, any queries to subdomains such as any.myhost.dyndns.org will be routed to myhost.dyndns.org.
Mail Exchanger	The Mail Exchanger (MX record) indicates in the Domain Name Service to which IP address or to which domain name E-mails for the configured DynDNS subdomain are to be sent. The specified destination address must be the address of a mail server.
Backup MX	If you enable this option, E-mails which are not delivered to the specified Mail Exchanger because it is temporarily not available, will be buffered by the DynDNS service and will finally be delivered once your Mail Exchanger is available again.
Use HTTPS for Update	If this option is enabled, the secure encrypted HTTPS connection is selected for updating.

28.3.1.14 Basic Settings > DynDNS > Update Timer DNS Names

Parameter Description of Tabs::

- **Edit Update Timer**

Parameters	Description
Update DNS Names	This option applies only to VPN. After the time interval set under "Update Timer value for DNS Names" expires, the VPN component checks whether any DNS names in the VPN configuration are resolved into new IP addresses (VPN with dynamic IP addresses). If this is the case, the VPN will be reconfigured with the new IP addresses.

Parameters	Description
Update Timer value for DNS names (sec)	Number of seconds for the interval between two updates. Value range: 60 to 1800, default value: 180

28.3.1.15 Basic Settings > Quality of Service

In the case of IP data traffic, the IP packets generated by the communication system are split into five groups. You can set which codepoint is to be used for marking the packets for four of these groups. The remaining data traffic is not prioritized (that is 00).

Priority class	ToS value, binary	ToS value, hexadecimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
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
Manual entry	xxx-xxx-00	0-63 (decimal)

Parameter Description of Tabs:

- **Edit Quality of Service Settings**

Parameters	Description
Priority Class for Signaling Data	Call signaling for connection setup with H.323/SIP Default value: AF31
Priority Class for Fax/ Modem Payload	Data Payload, for example, for IP networking with fax or modem Default value: EF
Priority Class for Network Control	Network Control, for example, SNMP traps Default value: CS7
Priority Class for Voice Payload	Voice Payload for IP telephony (Voice over IP) Default value: EF

28.3.1.16 Basic Settings > Date and Time > Date and Time

Parameter Description of Tabs::

- **Set Date and Time**

Parameters	Description
Date and Time	
Day	Selection of the day.
Month	Selection of the month.
Year	Entry of the year.
hh:mm:ss	Entry in the time in 24-hour format

28.3.1.17 Basic Settings > Date and Time > Timezone Settings

Parameter Description of Tabs::

- **Edit Timezone Settings**

Parameters	Description
Time zone	Local time zone in which the system is located

28.3.1.18 Basic Settings > Date and Time > SNTP Settings

Parameter Description of Tabs:

- **Edit Settings**

Parameters	Description
SNTP Client Input of access data for an external time server (SNTP) for network-wide synchronization of the system clock.	
Administration Mode of the SNTP Client	Enable or disable connection of the communication system to the SNTP server Default value: down
IP address/DNS name of External Time Server	IP address or DNS name of the SNTP server Default value: 0.de.pool.ntp.org
Poll Interval for External Time Server	Interval for the synchronization of the date and time with the SNTP server. Default value: 4 hours.

28.3.1.19 Basic Settings > Port Management

The displayed ports are used to identify the network protocols and appropriate network services. Some of the ports used by the communication system itself can be changed here. This enables the network communication to be customized for each customer network if the ports are already being used elsewhere. If changes are to be made at the port administration, these changes must generally be made in all components (phones, systems, etc.) simultaneously in order to retain functionality.

Parameter Description of Tabs::

- **Edit Global Port Management Settings**

Parameters	Description
Protocol Name	Service.
Port Number	Port n umber of the service (configurable).
Port type	The port type is displayed for information purposes; Single: a single port; Min: lower limit for a port range.
Services	
CSP	CSTA Service Provider, IP port for all applications that want to connect to the CSP. Default value: 8800
HFA	Control of HFA clients (CorNet-TC server port). Default value: 4060
HFA_EXT	Control of HFA clients (CorNet-TC server port) for System Device@Home. Default value: 4062
HFA_TLS	CorNet-TC via TLS. Default value: 4061
HFA_TLS_EXT	CorNet-TC via TLS for System Device@Home. Default value: 4063

Parameters	Description
MEB_SIP	MediaExtensionBridge, call signaling for SIPQ trunking. Default value: 15060
RTP_MIN	RTP/RTCP and T.38 ports (MediaBasePort). Default value: 29100
SIP	Call signaling for SIP telephones and SIP-based trunking. Default value: 5060
SIP_EXT	Call signaling for SIP telephones and ITSP trunking for SIP Device@Home. Default value: 5070
SIPS	Secure call signaling for SIPQ trunking. Default value: 5061
SIP_TLS_SUB	Secure call signaling for SIP stations. Default value: 5062
SIP_TLS_SUB_EXT	Secure call signaling for SIP stations for SIP Device@Home. Default value: 5071
VSL_MULTISITE	Multi-site connections. Default value: 8778

28.3.1.20 Basic Settings > Call Charges > Call Charges - Output Format

Parameter Description of Tabs::

- **Edit Output Format**

Parameters	Description
Format of Call Records	
Compressed Output Format	Default value: enabled
Last 4 digits suppressed	Replace the last 4 digits of the phone number field by question marks for privacy protection. Default value: disabled
Log incoming calls	Default value: disabled
Call Duration	Logging of call duration in hours, minutes, and seconds. Default value: enabled
On Ringing	For incoming calls, a call record is created immediately after the start of the call so that additional information on the caller can be transmitted for a caller list, for example or via a PC-based evaluation of the record. Default value: disabled

Parameters	Description
Output MSN	Logging of the used MSN (only IDSN) Default value: disabled
Decimal format	(Not in the USA) Format of the Advice of Charges; to be configured individually for each country. In Germany, the decimal format is always used. This decimal format also means that the multiplier is shown in hundredths. The multiplier specifies the amount by which the call charge unit is multiplied in order to obtain the currency value (e.g., 0.06 euro instead of 6 cents). Default value: enabled
Display amounts instead of units	Currency amounts are output instead of call charge units (e.g., 4.50 EUR instead of 75 units). Default value: enabled
Outgoing without connection	Logging of outgoing calls that were not answered. Default value: disabled
Outgoing LCR number outgoing or dialled number incoming	If this flag is activated, an additional phone number field is added to the call data record. It contains: • for an outgoing call: the LCR phone number that was actually sent to the exchange following conversion by LCR or • for an incoming call: the internal phone number of the station required, that is, the first station dialed. A call record is then output, even if a call is made for a busy station. This call record has the same format as the data record created for a free station except that the ring/call duration is set to "0". Default value: disabled
Call Detail Recording Central (CDRC)	
Output : none	No transmission of connection data Default value: HTTP
Output: HTTPS	Transmission of connection data to the supplied Call Charge Manager (Accounting Manager) or some other accounting software Default value: HTTP
Output : LAN TCP Client	Transmission of connection data to external server via TCP/IP Default value: HTTP
TCP client	Set IP address and port number of an external call charge server. If call charges have been incurred, a TCP/IP connection to the external call charge server (external application) is initiated by the communication system. When the connection has been set up, the call charge data is transmitted. The connection remains permanently open, and any other charges that occur are transmitted. transmitting each data record separately.

28.3.1.21 Basic Settings > Call Charges > Call Charges - Factors

Parameter Description of Tabs::

- **Edit Factors**

Parameters	Description
Call charge factor per direction	The call charge information can be offered in the form of call charge units (pulse counts) or currency units (cash amounts). Both forms are supported, but only currency units are displayed. If the information is received in the form of call charge units, a conversion factor is used. These call charge factors are set fees per direction and apply to both trunk calls (outside calls) as well as incoming and outgoing calls in the internetwork.
Routes	Displays the existing routes in the system
Multiplier	This multiplier is used for the conversion of tariff units to currency amounts. Value range: 0 to 65534, default value: 6
Multi-ISDN	Factor for converting currency amounts received or of Originals-based unit, and vice versa. Only for routes with the QSIG protocol. Value range: 1 to 65535, default value: 6
Currency	Abbreviation of the currency, e.g., EUR. This must be adjusted in line with the connected communication system. Currency string configuration is independent of the currency string shown on the telephone display. Note: This parameter is only significant for routes that use the QSIG protocol. This parameter is not applied for other protocols. The preset default setting must be retained in such cases. Value range: max. 3 characters
charges	You can use the charges column to define whether currency charges or call charge units are exchanged on the trunk. If this option is activated, the currency amount is sent and received (see the column Multi-ISDN). Otherwise, call charge units are sent and received. This must be adjusted in line with the connected communication system. If call charge pulses are to be exchanged on the route, an empty string should be configured as the currency. Note: This parameter is only significant for routes that use the QSIG protocol. This parameter is not applied for other protocols. The preset default setting must be retained in such cases.
Advice of charge: No charges	No charges are received via the route (e.g., US CO trunks). The parameter is not relevant for routes with the QSIG protocol.
Advice of charge: Interim	Charges are only received while the connection is active, and not during cleardown.
Advice of charge: Final	Charges are only received after the connection has been cleared down.
Advice of charge: Interim/ Final	Charges are received while a connection is active and during connection cleardown.
Currency	Currency code for the call charge display on telephones.

Parameters	Description
Computing accuracy	The computing accuracy of the communication system should be set to at least match that of the currency amounts transmitted by the CO. If the maximum of three decimal places is insufficient, the system automatically rounds up the number to the next unit. "Via call charge pulse" must be selected for routes with the QSIG protocol.

28.3.1.22 Basic Settings > Call Charges > Call Charges - Account Codes

Parameter Description of Tabs::

- **Change Account Codes**

Parameters	Description
Checking procedure	
Checking procedure: No check	The entered account codes are not checked. This option is not possible if there are routes with a mandatory entry procedure.
Checking procedure : List check	The entered account codes are checked for validity based on account code lists.
Checking procedure : Check number of characters	The entered account codes are checked for the number of characters.
Characters to be checked	Valid number of characters for the account code. Value range: 1 to 11, default value: 5
Account code lists	
List	A maximum of 1000 account codes can be entered for the list check.
Account code	Value range: max. 11 digits

28.3.1.23 Basic Settings > Announcement Player for Voicemails/Announcements

Parameter Description of Tabs:

- **Change announcement player for voicemails/announcements**

Parameters	Description
Voicemail	
Prefix	Call number for the voicemail box.
Announcement Player	
Call number	Call number of the announcement player.

28.3.1.24 Basic Settings > Phone Parameter Deployment

Parameter Description of Tabs:

- **Edit Phone Parameter Deployment**

Parameters	Description
Phone Parameter Deployment	
The following prerequisites must be satisfied for this parameter to be effective: the system telephones must use the DLI of the system, and the DLI must be able to supply the system telephones with the required parameters. The parameters of the system telephones are updated as soon as a system phone reconnects to the system or is restarted, or whenever the system is rebooted. The individual parameters can be configured directly at the system telephone or with the WBM of the system telephone. The settings for the PC Ethernet port and for the codec prioritization are not overwritten by the DLI if they were configured directly at the system telephone or with the WBM of the system telephone.	
activate Phone Parameter Deployment	If this flag is enabled, the options below are active for editing.
Deploy SW to @Home devices	If this flag is enabled, permissions are given for software update via DLI for HFA@Home devices.
Phone Parameter Settings	
Phone settings below may be changed here.	
PC port	If this flag is enabled, the PC Ethernet port is switched on at all active system telephones. Default: disabled
Codec setting is "low bandwidth preferred"	If this flag is enabled, the following codec prioritization applies to all system telephones: G.729 - G.711 - G.722 If this flag is disabled, the following codec prioritization applies: G.722 - G.711 - G.729 **NOTICE:** CP100 does not support G.722 Default: disabled
Display calling party images	If this flag is enabled, the caller's image appears on system telephones with a large color display on receiving an incoming call, provided the image was loaded into the system via UC Smart or UC Suite. Default: disabled
Apply Phone Parameter Settings	
Apply phone parameter settings to all phones	If this flag is enabled, all local administered settings are overwritten. Default: disabled

Parameter Description of Tabs:

- **Device Info**

  Following information for any device are mentioned here:

  Call number, Display, Device Type, IP Address, MAC Address, Current SW Version, HW Version, PC Port, Codec Setting.

Parameter Description of Tabs:

- **Change Admin Password**

  The administrator can configure the password for accessing to a phone's WBM.

Parameters	Description
The following prerequisites must be satisfied for this parameter to be effective: the system telephones must use the DLI of the system, and the DLI must be able to supply the system telephones with the required parameters.	
Change Admin Password	
The default password can be changed centrally for all DLI connected devices by the administrator.	
Password	The password must be entered in this field. The length of the password must be at least 6 characters.
Confirm Password	The password must be repeated in this field for verification purposes.

Parameter Description of Tabs:

- **Canonical Dial Settings**

  The administrator can distribute in bulk the canonical dial settings to all Desk Phone CP HFA devices which have DLI configured.

  Please note that the Canonical Dial Settings values, configured in WBM, will always overwrite the local (phone) settings.

Parameters	Description
Canonical Dial Settings	
Local country code	Required - Internal code for phone location. If not set then conversion will not take place. Maximum length: 5 characters.
National prefix digit	Needed - trunk prefix digit for PSTN dialling within the local country. Value: Maximum length: 5 characters.
Local National code	Needed - PSTN area code for the phone's location. Maximum length 6 characters.
Minimal local number length	Needed - PSTN local area length of numbers. Range: 0-50
Maximum local number length	Optional- PSTN local area length of numbers. A value of 0 means that this new rule will not be applied. Range: 0-50
Local Enterprise node	Optional - Local enterprise network code prefix for a phone as an extension. Maximum length 10 characters.
PSTN access code	Optional – list of digits to get PSTN access. Maximum length 10 characters.
International access code	Needed - list of PSTN access codes for the international gateway. Maximum length 5 characters.

Parameters	Description
Operator code	Optional - list of extensions numbers for operators. Maximum length 50 characters.
Emergency numbers	Optional - list of numbers that are used for emergency calls. Maximum length 50 characters.
Initial extension digits / Initial digits	Optional - List of initial digits for extension in the local enterprise network (defined by the local enterprise node). Maximum length 50 characters.
Expect dial number	Optional – Boolean to indicate when a PSTN access code + National prefix digit is retained and not converted into the International access code. True/ False with default value as false.
Canonical Dial	
Internal numbers	Drop-down list with the following options: Local enterprise form (default), Always add node, Use external numbers. Integer.
External numbers	Drop-down list with the following options: Local public form (default), National public form, International public form. Integer.
External access code	Drop-down list with the following options: Not required (default), For external numbers. Integer.
International gateway code	Drop-down list with the following options: Use national code (default), Leave as +. Integer.
Canonical dial lookup	
Local code 1-5	Optional - a local node code in the enterprise network. Maximum length 10 characters.
International code 1-5	Optional - the international code equivalent for the Local code. Maximum length 30 characters.

28.3.1.25 Basic Settings > Power Management

Parameter Description of Tabs:

- **Power management on/off**

Parameters	Description
Power Management Power management can be enabled only if is the LAN interfaces of the system are in the Ethernet Link Mode **Auto**. In the low power mode, the LAN interfaces of the system automatically switch to the 100 Mbit/s full-duplex mode. The LAN interfaces of the connected infrastructure should also be in the autosense mode.	
Power management on/off	Switches the system to the low power mode.
Beginning of the low power mode	Start time of the low power mode
End of the low power mode	End time of the low power mode.
The IP bandwidth is reduced to 100 Mbit/s FDX	Displays the data rate in low power mode

28.3.1.26 Basic Installation> Mass Data

- Parameter Description of Tabs:

Parameter	Description
Port	Port number. Not editable field.
Validity	There are two types of validation, the Front End Consistency Check and the Back End Consistency Check: a. The **Front End Consistency Check** validates data presented in the fields of Mass data wizard window by checking for inconsistencies and conflicts. An instant red indication is displayed in the Validity field under the respective numbers. On mouse over a pop up window indicates which is the exact conflict. b. The **Back End Consistency Check** validates data presented in the Mass Data wizard comparing them to data that are not viewable bust exist in the database of the system. These include Group, MULAP, Voicemail, National and International Access, VSL numbers, Seizure Codes and Line Codes (i.e. trunk access).
CalIno	Internal call number of the station.
DID	DID number of the station.
Dual Mode No.	Mobile call number of the station.
UC Mobile No.	Personal mobile number of UC Smart or UC Suite user. The number is in canonical format, e.g.: +49 89 7007 100. This number is displayed in the **My Personal Details** view of the user on the **User Directory**.
Email address	Email address of the station.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
First Name	Freely selectable first name for the station.
Last Name	Freely selectable last name for the station.
Device Type	The device type assigned to the user. Not editable field.
Type	Type of the station.
Type: **No Port**	Call number is not yet assigned to any station.
Type: **System Client**	A system client is an IP station that can use all the features of the communication system via CorNet-IP (formerly called HFA system client).
Type: **SIP Client**	A SIP client is an IP station that uses the SIP protocol. It can access only limited functionality of the communication system via SIP.
Type: **Deskshare User**	A Deskshare User is an IP user who can log in at another IP system telephone (mobile login) and then use this phone as his or her own phone (including the call number).
Fax CalIno	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.

Parameter	Description
Access	Displays the physical interface at which the device is connected.
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Status	Displays the status of the device. Active or inactive.

28.3.2 Security

Security settings are grouped together under **Security**. These include settings for firewalls, filters, VPN, and SSL.

28.3.2.1 Security > Application Firewall

Parameter Description of Tabs:

- **Display Services**
- **Add Service**
- **Delete all Services**

Parameters	Description
Application Firewall	The Application Firewall is used to restrict access to specific services such as FTP or LDAP. It is disabled by default and can be enabled by defining appropriate rules. The following services can either be blocked or restricted to specific IP addresses or IP address ranges by the Application Firewall: **Service / Ports** HTTPS / 443 Postgres / 5432 LDAP / 389 Manager E / 7000 ssh (locked by default) / 22 FTP / 21, 40000 - 40040 OBSERVER / The OBSERVER service allowed access from an OpenScape Observer application that is no longer supported. Only the listed services can be blocked via a selection menu in Expert mode. Telephone features such as SIP, HFA, etc. cannot be blocked using the Application Firewall. A service can be selected multiple times; each time different IP restrictions can be specified. **NOTICE:** The Application Firewall, when enabled, does not block services by default until a rule for that service is added, at which point only IP addresses included in the rule can access that specific service. The Application Firewall may restrict access to inter-node features when the system is networked to other OpenScape Business systems. As an example the survivability feature requires the POSTGRES service to function correctly, in this case if a rule is added for the POSTGRES service manually add the IP addresses of the other OpenScape Business networked nodes to the POSTGRES rule to ensure correct operation of the survivability feature.
Rule Name	Given name for the rule
Rule activated	The rule is activated.
Lower Limit of Source IP Address Range	The lower limit of the blocked IP addresses.
Upper Limit of Source IP Address Range	The upper limit of the blocked IP addresses.

28.3.2.2 Security > Deployment and Licensing Client (DLSC)

To use DLS functions, for example, the communication system must allow the external DLS to access the configuration data. The communication system is

then operated as Deployment and Licensing Client. The external DLS server is set up under> Mainboard > DHCP Mode > DHCP Server> Global Settings.

Parameter Description of Tabs::

- **DLSC Basic Configuration**
- **Contact DLSC**
- **Reset DLSC Bootstrapping**

Parameters	Description
Status	
Secure Communication with DLS Client	Indicates whether (and to what extent) secure communication with the DLS client is enabled or disabled (0).
DLS Client	
Time interval for ContactMe Response	Default value: 0
PIN required for DLS Bootstrapping	Enhanced level of security via PIN entry on both sides
Bootstrap PIN	Value range: min. 8 to max. 32 characters
DLS Server	
IP address of DLS server	Input of the IP address of the external DLS server.
Port of DLS Server	Port of the external DLS Server Default value: 18443
Secure Port of DLS Server	Display the port number for a secure connection

28.3.2.3 Security > Deployment and Licensing Client (DLSC) > DLSC Client Certificate

Parameter Description of Tabs:

- **Certificate Information**

Parameters	Description
Certificate Type	Used to ensure secure initial contact between the communication system and the DLS
Serial Number of Certificate	Displays the specified serial number.
Serial Number of Certificate (hex)	Displays the specified serial number in hexademical form.
Type of Signature Algorithm	Displays the signature algorithm used Value range: sha256RSA, sha512RSA
Start Time of Validity Period (GMT)	Displays the start of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).

Parameters	Description
End Time of Validity Period (GMT)	Displays the end of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).
CRL distribution point	Displays the optional URL from where the Certificate Revocation Lists (CRL) will be distributed
Issued by CA	The Certification Authority that has signed the certificate
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Subject Name	Displays the name of the subject who requested the certificate according to the conventions of the X.509 standard (for example, enter DE for Germany in the Country (C) field)
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format
Public Key Encryption Data	Public key data of certificate used for encryption
Public Key Length	Value range: 1024, 1536, 2048
Public Key	Encryption using public keys that are confirmed by a third party in accordance with the X.509 standard. The high level of security is guaranteed by the fact that the decryption key must be individually redefined and is only saved at the user's facility.
Fingerprint	The public key used and the fingerprint are displayed in hexadecimal format.

28.3.2.4 Security > Deployment and Licensing Client (DLSC) > DLSC CA Certificate

Parameter Description of Tabs:

- **Certificate Information**

Parameters	Description
Certificate Type	Used to ensure secure initial contact between the communication system and the DLS.

Parameters	Description
Serial Number of Certificate	Displays the specified serial number.
Serial Number of Certificate (hex)	Displays the specified serial number in hexademical form.
Type of Signature Algorithm	Displays the signature algorithm used. Value range: sha256RSA, sha512RSA
Start Time of Validity Period (GMT)	Displays the start of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).
End Time of Validity Period (GMT)	Displays the end of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).
CRL distribution point	Displays the optional URL from where the Certificate Revocation Lists (CRL) will be distributed.
Issued by CA	The Certification Authority that has signed the certificate
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Subject Name	Displays the name of the subject who requested the certificate according to the conventions of the X.509 standard (for example, enter DE for Germany in the Country (C) field).
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format.
Public Key Encryption Data	Public key data of certificate used for encryption
Public Key Length	Value range: 1024, 1536, 2048
Public Key	Encryption using public keys that are confirmed by a third party in accordance with the X.509 standard. The high level of security is guaranteed by the fact that the decryption key must be individually redefined and is only saved at the user's facility.
Fingerprint	The public key used and the fingerprint are displayed in hexadecimal format.

Parameters	Description
Certificate Type	Used to ensure secure initial contact between the communication system and the DLS.

28.3.2.5 Security > Signaling and Payload Encryption

Parameter Description of Tabs:

- **Edit Security Configuration**

Parameters	Description
Minimum length of the RSA key:	Minimum length of the RSA key in the certificates. The higher the value, the more secure the key Value range: 512, 1024, 2048 Default: 1024
Certificate validation	Switches the certificate validation on or off completely. We recommend that you do not switch off the certificate validation. Default: on
Subject name check	By checking the subject name in the certificate of a gateway, its identity can be checked. The subject name contains the IP address or the DNS name (DNS: Domain Name System) of the respective gateway Default: disabled
CRL verification	Using a Certificate Revocation List (CRL), it is possible to determine whether a certificate was blocked/revoked and why. When a Certification Authority (CA) declares a certificate to be invalid, it enters the serial number of that certificate in its list. During certificate validation, this list can be checked at the Certification Authority via the Internet. Default: disabled
Enforce Secure Renegotiation (RFC 5746)	This procedure improves security during the renegotiation of the encryption parameters for TLS connections. It can only be used provided it is supported on all connected servers. (OpenScape Business, OpenScape 4000 and OpenScape Voice support this improved procedure; HiPath 3000 does not). Default: disabled
Maximum Re-Keying interval (hours)	This interval determines how long a specific key is to be used for the encryption of signaling and user data. After this period expires, a new key is defined. Value range: 6 to 48 Default: 24

28.3.2.6 Security > Signaling Encryption/Payload Encryption > SPE Certificate

Parameter Description of the Tab:

- **Import SPE certificate plus private key (PKCS#12 file)**

Parameters	Description
Passphrase for decryption	Input of the passphrase that was used when creating the PKCS#12 file.
File with certificate and private Key (PEM or PKCS#12 format)	Selection of the file containing the certificate data to be imported.

28.3.2.7 Security > Signaling Encryption/Payload Encryption > SPE CA Certificates

Up to 16 trusted CA certificates can be imported individually from a client PKI certificate authority (RA/CA), for example.

Parameter Description of the Tab:

- **Import trusted CA Certificate (X.509 file) for SPE**

Parameters	Description
File with certificate (PEM or binary)	Selection of the PEM or binary file to be imported.
CRL Distribution Point (CDP) Protocol	Protocol selection for the CRLs (certificate revocation lists) Value range: LDAP or HTTP
CDP (e.g., without ldap://)	A CDP is an optional certificate extension. An imported certificate is only checked against the CRLs for which the CDP was configured.

28.3.2.8 Security > VPN

Parameter Description of Tabs:

- **Display General Information**
- **Activate the Configured VPN Tables**
- **IPsec on / off**

Parameters	Description
Encryption Algorithms	Used encryption algorithms Value range: AES, 3DES
Hash Algorithms	Standardized cryptographic hash function used to compute a unique check value (digital signature) Value range: MD5, SHA1, SHA2
Public Key Algorithms	Asymmetric encryption method Value range: RSA
Diffie-Hellman Groups	A method for exchanging keys Value range: DH Group 2, DH Group 5
Buttons	

Parameters	Description
Activate Now	The VPN tables can be activated. Observe the warnings!
Activate/Deactivate IPsec	IPSec can be enabled or disabled. Observe the warnings!

28.3.2.9 Security > VPN > Lightweight CA

Parameter Description of Tabs:

- **Generate CA Certificate**

Parameters	Description
Name of the Certificate	Freely definable flat name for the generated certificate
Serial Number of Certificate	Input of a serial number that you specify. This number must be a positive integer.
Type of Signature Algorithm	Selection of the signature algorithm to be used for this certificate Value range: sha25RSA, sha512RSA
Public key length	Selection of a key length used for this certificate Value range: 2048
Start Time of Validity Period (GMT) Point of time as of which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).	
End Time of Validity Period (GMT) Point of time until which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).	
Subject Name Input of the subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field).	
Alternative Subject Name This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and some other format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured..	
Distinguished Name Format	This is usually also provided as the Common Name RDN within the Subject field of the main certificate
Other Format	Other names, given as a General Name
Subject Alternative Name Extension	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other

Parameters	Description
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured..
CRL Distribution Point Type	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
CRL Distribution Point	Specification of a URL from where the Certificate Revocation Lists (CRL) will be distributed.
Generate Certificate	

28.3.2.10 Security > VPN > Certificate Management

Parameter Description of Tabs::

- **View Certificate From File**

Parameters	Description
PKCS#12 Format	You must activate this field if the certificate is saved in a PKCS#12 file.
Passphrase for decryption	If you activate the PKCS#12 Format field, you must enter the same password in this field as used for file creation.
File with Certificate	Enter the path and the file name of the certificate in this field. Click on Browse if you are unsure of the storage location. A search dialog is displayed.

28.3.2.11 Security > VPN > Certificate Management > Trusted CA Certificates > Active Certificates

Parameter Description of the Tab:

- **Import Trusted CA Certificate (X.509)**

Parameters	Description
Certificate Type	Used to ensure secure initial contact between the communication system and the DLS
Serial Number of Certificate	Displays the specified serial number.
Serial Number of Certificate (hex)	Displays the specified serial number in hexademical form.
Type of Signature Algorithm	Displays the signature algorithm used Value range: sha256RSA, sha512RSA
Start Time of Validity Period (GMT)	Displays the start of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).

Parameters	Description
End Time of Validity Period (GMT)	Displays the end of the certificate validity period. The time specified is interpreted as Greenwich Mean Time (GMT).
CRL distribution point	Displays the optional URL from where the Certificate Revocation Lists (CRL) will be distributed
Issued by CA	The Certification Authority that has signed the certificate
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Subject Name	Displays the name of the subject who requested the certificate according to the conventions of the X.509 standard (for example, enter DE for Germany in the Country (C) field)
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format
Public Key Encryption Data	Public key data of certificate used for encryption
Public Key Length	Value range: 1024, 1536, 2048
Public Key	Encryption using public keys that are confirmed by a third party in accordance with the X.509 standard. The high level of security is guaranteed by the fact that the decryption key must be individually redefined and is only saved at the user's facility.
Fingerprint	The public key used and the fingerprint are displayed in hexadecimal format.

28.3.2.12 Security > VPN > Certificate Management > Trusted CA Certificates > Configured Certificates

Parameter Description of the Tab:

- **Import Trusted CA Certificate (X.509)**

Parameters	Description
Name of the Certificate	Enter the name to be assigned to the certificate.
File with Certificate	Path and file name of the certificate. When you click Browse, a search dialog is displayed to find the storage location of the file.

28.3.2.13 Security > VPN > Peer Certificates

Parameter Description of Tabs:

- **Generate Certificate Signing Request (CSR)**
- **Import Peer Certificate (PKCS#12)**

Parameters	Description
Certificate Request Name	A CA-signed peer certificate based on a CA certificate can be generated. This requires at least one CA certificate to have already been generated. The certificate generated is saved in a PKCS#12 file. PKCS#12 files (Personal Information Exchange Syntax Standard) save certificates with the private key. A PKCS#12 file therefore contains the necessary data for personal encryption and decryption.
Type of Signature Algorithm	Select the signature algorithm to be used for this certificate. Value range: sha25RSA, sha512RSA
Public key length	Value range: 2048
Subject Name	Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field).
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Alternative Subject Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured..
Distinguished Name Format	This is usually also provided as the Common Name RDN within the Subject field of the main certificate
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)

Parameters	Description
Other Format	Other names, given as a General Name
Subject Alternative Name Extension	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
Subject Alternative Name	This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format.
Import Peer Certificate [PKCS#12]	
Name of the Certificate	Enter the name to be assigned to the certificate.
Passphrase for decryption	Password to decrypt the peer certificate Value range: min. 7 and max. 32 characters
File with Certificate	Click on Browse. A search dialog is displayed.
View Fingerprint of Certificate	Click on this button to check the integrity of the certificate.
Import Certificate from File	Click on this button to import a certificate.

28.3.2.14 Security > VPN > Services > Active Services

Parameter Description of the Tab:

- **Display IPsec Services**

Parameters	Description
Name of the Service	This field contains the name of the configured services.
State in IP Stack	
Source Port	Displays the source port number. If "0" is displayed as the port, this corresponds to any (unknown) port.
Destination Port	Displays the destination port number. If "0" is displayed as the port, this corresponds to any (unknown) port.
IP protocol	Displays the IP protocol used for the transmission.
Associated 'pass' Rule	Displays the associated "Pass" rule. The assignment of rules and services is performed under Rules.
Associated 'deny' Rule	Displays the associated "Deny" rule. The assignment of rules and services is performed under Rules.

28.3.2.15 Security > VPN > Services > Configured Services

Parameter Description of Tabs::

- **Display IPsec Services**
- **Add IPsec Services**
- **Edit IPsec Services**
- **Rename IPsec Services**
- **Delete IPsec Services**

Parameters	Description
Name of the Service	Input field for the name of the newly configured service. Enter a character string in this field.
Source Port	Number of the port to be used for the transmission of data on the transmit side. In this field, "0" indicates any (unknown) port.
Destination Port	Number of the port to be used for the transmission of data on the receive side. In this field, "0" indicates any (unknown) port.
IP protocol	IP protocol to be used for the transmission Value range: ICMP, TCP, UDP
Name of the Service	Input field for the name of the service to be configured.
Source Port	Number of the port to be used for the transmission of data on the transmit side. In this field, "0" indicates any (unknown) port.
Destination Port	Number of the port to be used for the transmission of data on the receive side. In this field, "0" indicates any (unknown) port.
IP protocol	Select the IP protocol used for the transmission Value range: ICMP, TCP, UDP
Name of the Service	Input field for the name of the service to be configured.
	Deletion is only possible if no rule is assigned to the service.

28.3.2.16 Security > VPN > Tunnels > Active Tunnels

Parameter Description of Tabs::

- **Display General Tunnel Data**
- **Display Rules for all Tunnels**

Parameters	Description
Name of the Tunnel	This field contains the name of the configured tunnel.
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Type of the Local Tunnel Endpoint	Displays the endpoint address at the sending end of the tunnel; you can specify a host name or a DNS name).
Local Tunnel Endpoint Address	Displays the endpoint address in the local tunnel.

Parameters	Description
Type of the Remote Tunnel Endpoint	Displays the endpoint type of the remote tunnel.
Remote Tunnel Endpoint Address	Displays the recipient address of the remote tunnel. If the address of 0.0.0.0 is displayed, this means that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
Suggested Lifetime of the Session Keys	Displays the accepted validity period for the session keys which will be used. When this period expires, no more data is exchanged within this session. New session keys are automatically negotiated to replace invalid session keys.
Suggested Lifetime of the Key Exchange Session	Displays the accepted validity period for the key exchange session. Once the key exchange session has expired, new keys are automatically negotiated for it using the IKE protocol (encryption protocol).
Associated Rules: Associated Transmit Rule	Setup of Send Rules under VPN > Rules
Associated Rules: Associated Receive Rule	Setup of Receive Rules under VPN > Rules
Tunnel Data	
Name of the Tunnel	This field contains the name of the configured tunnel.
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Type of the Local Tunnel Endpoint	Displays the endpoint address at the sending end of the tunnel; you can specify a host name or a DNS name).
Local Tunnel Endpoint Address	Displays the endpoint address in the local tunnel.
Type of the Remote Tunnel Endpoint	Displays the endpoint type of the remote tunnel.
Remote Tunnel Endpoint Address	Displays the recipient address of the remote tunnel. If the address of 0.0.0.0 is displayed, this means that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
Rule Data	
Destination	Status indicator in the Destination. Value range: send/ receive
Priority	Displays the priority for the processing sequence. The highest priority is specified with 1. Each rule associated with a direction must be assigned its own priority. A rule and the associated opposite-direction rule must always have the same priority. The rule for the opposite direction can only be created with the corresponding menu item.
Rule-Based Action	Displays how the IP packets are to be handled by the rule: "pass" means that IP packets are forwarded; "deny" means that no IP packets are forwarded.
Encryption Required	Displays an encryption for this rule. The encryption procedure is defined by the assigned tunnel.

Parameters	Description
Rule State	Status indicator in the rule. Value range: enabled/ disabled
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Source Address Displays the source and destination address in a format suitable for the selected type. The display depends on the selected address type. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.	
Type	Displays the type of the source address and destination address (possible values are: host, subnet, IP address range and DNS name).
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Destination Address	
Type	Displays the type of the source address and destination address (possible values are: host, subnet, IP address range and DNS name).
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Service Data Displays the service to which the encryption is restricted. If the encryption is not to be restricted to one service, select "Any Service"	
Name of the Service	Input field for the name of the service to be configured.
Source Port	Displays the tunnel in the receive direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Select No Tunnel Assignment if no tunnel is to be assigned in the receive direction.

Parameters	Description
Destination Port	Displays the tunnel in the send direction, to which this rule applies. IP packets destined for the network are sent through this tunnel. Select No Tunnel Assignment if no tunnel is to be assigned in the send direction.
IP protocol	Select the IP protocol used for the transmission Value range: ICMP, TCP, UDP

28.3.2.17 Security > VPN > Tunnels > Configured Tunnels

Parameter Description of Tabs::

- **Display General Tunnel Data**
- **Display Rules for all Tunnels**
- **Add Tunnel / Edit Tunnel Data**
- **Key exchange data**

Parameters	Description
	Tunnel is the term used to describe the transportation of encrypted data packets to a defined endpoint. Active tunnels become configured tunnels when the configuration is enabled. A maximum of 256 tunnels can be set up per gateway.
Name of the Tunnel	This field contains the name of the configured tunnel.
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Type of the Local Tunnel Endpoint	Displays the endpoint address at the sending end of the tunnel; you can specify a host name or a DNS name).
Local Tunnel Endpoint Address	Displays the endpoint address in the local tunnel.
Type of the Remote Tunnel Endpoint	Displays the endpoint type of the remote tunnel.
Remote Tunnel Endpoint Address	Displays the recipient address of the remote tunnel. If the address of 0.0.0.0 is displayed, this means that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
Suggested Lifetime of the Session Keys	Displays the accepted validity period for the session keys which will be used. When this period expires, no more data is exchanged within this session. New session keys are automatically negotiated to replace invalid session keys.
Suggested Lifetime of the Key Exchange Session	Displays the accepted validity period for the key exchange session. Once the key exchange session has expired, new keys are automatically negotiated for it using the IKE protocol (encryption protocol).
Associated Rules: Associated Transmit Rule	Setup of Send Rules under VPN > Rules
Associated Rules: Associated Receive Rule	Setup of Receive Rules under VPN > Rules

Parameters	Description
Tunnel Data	
Name of the Tunnel	This field contains the name of the configured tunnel.
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Type of the Local Tunnel Endpoint	Displays the endpoint address at the sending end of the tunnel; you can specify a host name or a DNS name).
Local Tunnel Endpoint Address	Displays the endpoint address in the local tunnel.
Type of the Remote Tunnel Endpoint	Displays the endpoint type of the remote tunnel.
Remote Tunnel Endpoint Address	Displays the recipient address of the remote tunnel. If the address of 0.0.0.0 is displayed, this means that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
Rule Data	
Destination	Status indicator in the Destination. Value range: send/ receive
Priority	Displays the priority for the processing sequence. The highest priority is specified with 1. Each rule associated with a direction must be assigned its own priority. A rule and the associated opposite-direction rule must always have the same priority. The rule for the opposite direction can only be created with the corresponding menu item.
Rule-Based Action	Displays how the IP packets are to be handled by the rule: "pass" means that IP packets are forwarded; "deny" means that no IP packets are forwarded.
Encryption Required	Displays an encryption for this rule. The encryption procedure is defined by the assigned tunnel.
Rule State	Status indicator in the rule. Value range: enabled/ disabled
State in IP Stack	Status indicator in the IP stack. Value range: active / not active
Source Address Displays the source and destination address in a format suitable for the selected type. The display depends on the selected address type. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.	
Type	Displays the type of the source address and destination address (possible values are: host, subnet, IP address range and DNS name).

Parameters	Description
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Destination Address	
Type	Displays the type of the source address and destination address (possible values are: host, subnet, IP address range and DNS name).
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Service Data Displays the service to which the encryption is restricted. If the encryption is not to be restricted to one service, select "Any Service"	
Name of the Service	Input field for the name of the service to be configured.
Source Port	Displays the tunnel in the receive direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Select No Tunnel Assignment if no tunnel is to be assigned in the receive direction.
Destination Port	Displays the tunnel in the send direction, to which this rule applies. IP packets destined for the network are sent through this tunnel. Select No Tunnel Assignment if no tunnel is to be assigned in the send direction.
IP protocol	IP protocol to be used for the transmission Value range: ICMP, TCP, UDP
Name of the Tunnel	This field contains the name of the newly configured tunnel.
Enable Remote Service via VPN : (can be activated via the service code)	Check this box if the VPN tunnel is to be used for remote administration.
Type of the Local Tunnel Endpoint	Select the endpoint address type at the sending end of the tunnel; you can specify a host name or a DNS name.
Local Tunnel Endpoint Address	Enter the sender's address in a format suitable for the endpoint type.

Parameters	Description
Type of the Remote Tunnel Endpoint	Type of endpoint address on the tunnel receive side (specification of IP address is supported).
Remote Tunnel Endpoint Address	Receive address in a format suitable for the endpoint type. In this field, 0.0.0.0 indicates that the tunnel endpoint is unknown. In this case, the tunnel must be configured by the peer (e.g. teleworker).
Session Key Handling	Under Session Key Handling, specify the procedure for the key exchange (Automatically, using IKE protocol).
Suggested Encryption Algorithms	Which algorithms may be used Value range: AES, 3DES
Suggested Hash Algorithms	Which hash algorithms (testing algorithms) may be used. The selected algorithms are offered by the initiator of IKE negotiation. Value range: MD5, SHA1, SHA2
Suggested Lifetime of the Session Keys	Validity period for the session keys that are used. When this period expires, no more data is exchanged within this session. New session keys are automatically negotiated to replace invalid session keys
Suggested Lifetime of the Key Exchange Session	Validity period for the key exchange session. Once the key exchange session has expired, new keys are automatically negotiated for it using the IKE protocol
Suggested Data Volume of the Session Keys	Maximum data volume for the session keys. If the data volume is exceeded, new session keys are automatically negotiated using the IKE protocol. If "unlimited" is selected, the amount of data is unrestricted
Activate Perfect Forward Secrecy	It is recommended to always select this option, since it activates improved security mechanisms for data transfer via the tunnel
VPN Peer Authentication Method	VPN subscriber authentication method. The possible options include Digital Signatures (authentication using certificates) and Pre-Shared Keys (authentication using self-defined manual keys)
Pre-Shared Key	This field is only available if the authentication method is set to Pre-Shared keys. The password to be used by the VPN subscribers at both endpoints of the tunnel must be entered here. At least 12 characters should be used
Reenter Pre-Shared Key	This field is only available if the authentication method is set to Pre-Shared keys.
List of CA Certificates	These options are only available if the authentication method is set to Digital signatures. For authentication, VPN subscribers can use any certificate that has been issued (signed) by one of the selected CA certificates
Suggested Diffie-Hellman Groups	VPN subscribers can exchange keys by any of the selected methods

NOTICE: The addition/deletion of a VPN tunnel must subsequently be enabled under "VPN> Activate the Configured VPN Tables".

28.3.2.18 Security > VPN > Rules > Active Rules

Parameter Description of the Tab:

- **Display Rules**

Parameters	Description
Priority	Displays the priority for the processing sequence as a digit. The highest priority is specified with 1. Each rule associated with a direction must be assigned its own priority. A rule and the associated opposite-direction rule must always have the same priority.
Service	Displays the service to which the encryption is restricted. If the encryption is not restricted to one service, "Any Service" is displayed.
Rule-Based Action	Displays how the IP packets are to be handled by this rule: "pass" means that IP packets are forwarded; "deny" means that no IP packets are forwarded.
Encryption Required	Displays the encryption. The encryption procedure is defined by the assigned tunnel.
Rule State	Status indicator in rule. Value range: Enabled / Disabled
State in IP Stack	Status indicator in the IP stack. Value range: Enabled / Disabled
Source Address	
Type	Displays the type of the source address. Value range: Host, Subnet, IP Address Range, DNS Name
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Destination Address	
Type	Displays the type of the destination address. Value range: Host, Subnet, IP Address Range, DNS Name
Address (Highest in Range)	
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Tunnels for Encryption	

Parameters	Description
Tunnel on Receive Side	Displays the tunnel in the receive direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Display: No Tunnel Assignment (if no tunnel was assigned in the receive direction).
Tunnel on Transmit Side	Displays the tunnel in the send direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Display: No Tunnel Assignment (if no tunnel was assigned on the transmit side).

28.3.2.19 Security > VPN > Rules > Configured Rules

Rules define how IP packets are to be handled. The rule action Pass means that the IP packet is to be transported further (passed through). The rule action Deny means that the IP packet will not be transported further (i.e., will be ignored). You can also select whether or not the IP packet will use an encrypted VPN tunnel. The communication system can manage 640 rules, of which 6 rules are preset (default rules) and 634 are free for allocation.

Parameter Description of Tabs::

- **Display Rules**
- **Add Rule**
- **Edit Rule**
- **Add Rule for Opposite Direction**
- **Delete Rule**

Parameters	Description
Priority	Displays the priority for the processing sequence as a digit. The highest priority is specified with 1. Each rule associated with a direction must be assigned its own priority. A rule and the associated opposite-direction rule must always have the same priority.
Service	Displays the service to which the encryption is restricted. If the encryption is not restricted to one service, "Any Service" is displayed.
Rule-Based Action	Displays how the IP packets are to be handled by this rule: "pass" means that IP packets are forwarded; "deny" means that no IP packets are forwarded.
Encryption Required	Displays the encryption. The encryption procedure is defined by the assigned tunnel.
Rule State	Status indicator in the rule. Value range: enabled/ disabled
State in IP Stack	Status indicator in the IP stack. Value range: Enabled / Disabled
Source Address	
Type	Displays the type of the source address. Value range: Host, Subnet, IP Address Range, DNS Name

Parameters	Description
Address (Lowest in Range)	Displays the source and destination address in a format suitable for the selected type. The input mask depends on the address type selected. If any IP address is to be used, 0.0.0.0 is displayed. NAT must be deactivated at the interface to the destination network if 0.0.0.0 is specified as the destination IP address for transmitting packets in a tunnel. Alternatively, you can specify an IP address between 0.0.0.1 and 255.255.255.254 to transmit packets in a tunnel.
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Destination Address	
Type	Displays the type of the destination address. Value range: Host, Subnet, IP Address Range, DNS Name
Address (Highest in Range)	
Subnet Mask / Highest Addr. in Range	It is set in case that a range of source/destination addresses need to be set for transmission
Tunnels for Encryption	
Tunnel on Receive Side	Displays the tunnel in the receive direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Display: No Tunnel Assignment (if no tunnel was assigned in the receive direction).
Tunnel on Transmit Side	Displays the tunnel in the send direction, to which this rule applies. IP packets received by the network are retrieved from this tunnel. Display: No Tunnel Assignment (if no tunnel was assigned on the transmit side).

28.3.2.20 Security > VPN > Public Key Infrastructure (PKI)

The PKI server designates a server that can issue, distribute and verify digital certificates. The certificates issued within a PKI (Public Key Infrastructure) are used to protect communications. When using certificates (digital signatures), an attempt is made to download the CRL via the PKI URL configured by the PKI server.

Parameter Description of Tabs::

- **Display PKI Servers**
- **Add PKI Server**

Parameters	Description
Name of the PKI Server	Enter an easily recognizable name for the server.
PKI Server Type	Select the task of the server (you can choose between LDAP and Enrollment).
URL of the PKI Server	Enter the URL of the server (for example: LDAP://139.21.92.144:389).

28.3.2.21 Security > SSL > Certificate Generation

Administrative access is encrypted over HTTPS using the TLS 1.2 protocol. Certificates are used to authenticate the connection. By default, a self-signed certificate is used. A customer-specific certificate issued by a certificate authority (CA) can be used to enhance security. The communication system uses the certificates generated or imported by the WBM for authentication at the admin client. Such certificates can be imported into the browser as trusted certificates to avoid warning messages in the browser when connecting to the SSL server.

Parameter Description of Tabs:

- **Generate CA Certificate**
- **Generate Self-Signed Certificate**

Parameters	Description
Name of the Certificate	Name of the certificate to be generated.
Serial Number of Certificate	Serial number for the certificate. This number must be a positive integer
Type of Signature Algorithm	Signature algorithm to be used Value range: sha256RSA, sha512RSA
Public Key Length	Value range, default value: 2048
Start Time of Validity Period (GMT) Point of time as of which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT).	
Day, Month, Year, Hrs, Mins, Sec.	Time specification units for the certificate validity period
End Time of Validity Period (GMT) Point of time until which the certificate should be valid. The time specified is interpreted as Greenwich Mean Time (GMT)	
Day, Month, Year, Hrs, Mins, Sec.	Time specification units for the certificate validity period
Subject Name Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field). All four fields must be filled.	
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)

Parameters	Description
Alternative Subject Name	
This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format.If other format is selected, more than one SAN entries is possible to be configured..	
Distinguished Name Format	This is usually also provided as the Common Name RDN within the Subject field of the main certificate
Other Format	Other names, given as a General Name
Subject Alternative Name Extension	(optional)Value range, default value: DNS Name, IP Address, E-mail Address, Uniform ResourceIndicator, Other
Subject Alternative Name	
CRL Distribution Point Type	Value range: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
CRL Distribution Point	The location from which certificate revocation lists (CRL) are to be distributed can be optionally specified here (with a URL)

28.3.2.22 Security > SSL > Certificate Management

Parameter Description of the Tab:

- **View Certificate From File**

Parameters	Description
PKCS#12 Format	This field must be activated if the certificate is saved in a PKCS#12 file.
Passphrase for decryption	If the PKCS#12 Format field was activated, the same password that was used when creating the file must be entered in this field.
File with Certificate	Enter the path and file name of the certificate. If necessary, click Browse to specify the location.

28.3.2.23 Security > SSL > Certificate Management > Server Certificates

Parameter Description of Tabs:

- **Generate Certificate Signing Request (CSR)**
- **Import Server Certificate (PKCS#12)**
- **View a Certificate**
- **Remove Certificate**
- **Export Certificate (X.509)**
- **Import Updated Certificate (X.509)**
- **Activate Certificate**

Parameters	Description
Certificate Request Name	Name of the certificate to be generated.

Parameters	Description
Type of Signature Algorithm	Signature algorithm to be used for this certificate Value range: sha256RSA, sha512RSA
Public Key Length	Value range: 2048
Subject Name Subject name data of the certificate applicant according to the conventions of the X.509 standard (e.g., DE for Germany in the Country (C) field). All four fields must be filled.	
Country (C)	Two-digit country code
Organization (O)	The full legal company name
Organization Unit (OU)	The Organizational Unit is whichever branch of the company is ordering the certificate
Common Name (CN)	Fully Qualified Domain Name (FQDN)
Alternative Subject Name This optional information distinguishes between the Distinguished Name Format (such as the data under Subject Name) and Other Format (for example, the IP address entry). The input mask depends on the selected format. If other format is selected, more than one SAN entries is possible to be configured..	
Distinguished Name Format	This is usually also provided as the Common Name RDN within the Subject field of the main certificate
Other Format	Other names, given as a General Name
Subject Alternative Name Extension	(optional) Value range, default value: DNS Name, IP Address, E-mail Address, Uniform Resource Indicator, Other
Subject Alternative Name	(optional)
Name of the Certificate	Name of the certificate to be imported.
Passphrase for decryption	Password that was used when the file was created. Value range: 7 to 32 characters
File with Certificate	Enter the required certificate in the **File with Certificate** field or select it using Browse. The **Fingerprint** of the certificate must displayed first and can then be imported.

28.3.2.24 Security > Web Security

Parameter Description of the Tab:

- **Web Access Filter**

Parameters	Description
Web Clients	Only in conjunction with UC Suite: Enabling and disabling web access from mobile phones and mobile applications (myPortal for Mobile/Tablet, myPortal to go, Application Launcher and 3rd party applications via a Web Service) Info: Use of web clients in conjunction with UC Smart via Expert mode > Applications > UC Smart > Basic Settings
Access via HTTPS	Only encrypted connections allowed.
Access via HTTP	Unencrypted connections are allowed.
Save login data for devices	When enabled, login credentials do not need to be entered whenever the application is started

28.3.2.25 Security > SQL Security

Parameter Description of the Tab:

- **SQL Access Password**

Parameters	Description
Generate New	An encrypted SQL password, not known to the user, is generated.
Activate default	The default SQL password is activated.

28.3.3 Network Interfaces

Functions such as the configuration of the individual interfaces are grouped together under **Network Interfaces**. The interfaces can be configured separately.

28.3.3.1 Network Interfaces > Mainboard > Host Name

Parameter Description of Tabs::

- **Editing the Host Name**

Parameters	Description
Host Name	Host name of the communication system - optional. Example: `commsystem` If the name and IP address of the communication system are stored on a DNS server, name resolution can occur. The name of the communication system is composed of the host name and the domain name. Example: `commsystem.mynet.home`

28.3.3.2 Network Interfaces > Mainboard > LAN 1 (WAN)

Parameter Description of Tabs:

- **Show LAN 1 Mode**
- **Edit LAN 1 Interface**
- **Edit ACD**

Parameters	Description
Internet Service Provider Selection	Selection to determine how access to an ISP (Internet Service Provider) via the WAN interface occurs.
Internet Service Provider Selection: Not configured or disabled	The WAN interface is not used.
Internet Service Provider Selection: LAN Connection Type TCP/IP	The WAN interface is used for access to an ISP, which is already configured in an external Internet router. The communication system and Internet router do not need to be on the same LAN segment, but the WAN interface must be connected to the LAN segment of the Internet router.
Internet Service Provider Selection: T-Online, T-DSL Business, …	The communication system functions as an Internet router. The WAN interface is used for access to a preconfigured ISP.
Internet Service Provider Selection: Provider PPPoE	The communication system functions as an Internet router. The WAN interface is used for access to an ISP using PPPoE. PPPoE is the protocol most commonly used by DSL modems.
Internet Service Provider Selection: Provider PPTP	The communication system functions as an Internet router. The WAN interface is used for access to an ISP using PPTP. This variant is common in Austria, for example.
Internet access via an external Router	Access to the Internet occurs via an external router. This flag is internally used by the **Internet Configuration** wizard and should not be changed.
Automatic Address Configuration (via DHCP)	An external DHCP server (possibly the DHCP server of the Internet router) assigns an IP address to the communication system.
Accept IP Address of the Default Router	The external DHCP server communicates the IP address of the default router (e.g., the Internet router) to the communication system.
Accept IP Address of the DNS Server	The external DHCP server communicates the IP address of the DNS server to the communication system.
Accept IP Address of the SNTP Server	The external DHCP server communicates the IP address of the SNTP server to the communication system.
IP address	IP address of the LAN interface.
Subnet Mask:	Netmask of the LAN segment.
MAC Address	Displays the MAC address of the LAN interface.
Ethernet Link Mode	WAN interface mode.
Ethernet Link Mode: Auto	Automatic switching between 100 and 1000 Mbps full duplex mode.
Ethernet Link Mode: 100HDX	100 Mbps, full duplex.

Parameters	Description
Ethernet Link Mode: 100FDX	100 Mbps, full duplex.
Ethernet Link Mode: 1000FDX	1000 Mbps, full duplex.
NAT	NAT (Network Address Translation) is turned on. This task is usually already assumed by the external router.
Bandwidth Control for Voice Connections	This field enables bandwidth control for voice connections.
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.
Bandwidth Used for Voice/ Fax (%)	Percentage of bandwidth available for voice/fax connections. Value range, default value: 0 - 100, 80
IEEE802.1p/q Tagging	If this check box is selected, a "type of service" is included in the Ethernet packets (Layer 2) for prioritization purposes The option is deactivated by default.
IEEE802.1p/q VLAN ID	Enter the VLAN's ID number if the used switch has problems with the default value "0".
Layer 2 QoS Class	
Signaling Data	Priority class for the connection setup. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 3
Fax/Modem Payload	Priority class for the fax and modem data of the IP connection. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 5
Network Control	Priority class for the network control data (transfer of SNMP traps, for example). 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 0
Voice Payload	Priority class for the voice data of the IP connection. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 5
Internet Access Data for …	
Connection ID / User Name / T-Online number / Subuser Number/Suffix / Internet Access Account / DSL-Login …	Access data of the Internet Service Provider.
CHAP Password	Password for access to the Internet Service Provider.
Reenter Password	Password for access to the Internet Service Provider.
IP parameters	

Parameters	Description
Remote IP Address of the PPP Connection	IP address of the ISP server, if the ISP uses a static IP address.
Local IP Address of the PPP Connection	IP address that was assigned by your ISP for Internet access.
IP Address Negotiation	Selection to determine how the connection partners should negotiate the IP address at connection setup.
IP Address Negotiation: configured IP address	Only the configured IP address is possible.
IP Address Negotiation: accept any IP address	Any address proposed by the partner is accepted.
IP Address Negotiation: request new IP address	A new IP address is requested at each connection.
DNS Request	
Internet Access with DNS Request	The DNS server is determined automatically.
IP Address of primary DNS Server	A special DNS server is selected.
General PPP Parameters	
Default Router	The PPP connection created here is used as the routing destination.
IP Header Compression	The TCP header is compressed. UDP and RTP headers are always compressed.
Send LCP Echo Request	An LCP echo request is sent. This function is used to check if the connection is still active.
Automatic PPP Reconnection	The PPP connection is automatically reestablished after a connection cleardown (for example, in the case of ISP access with a flat rate and a forced disconnect after 24 hours).
PPTP Parameter	
Local IP Address of the Control Connection	IP address that was assigned by your ISP for the PPTP connection.
Remote IP Address of the Control Connection	IP address of your ISP's server for the PPTP connection.
Remote subnet mask for the control connection	Subnet mask that was assigned by your ISP for the PPTP connection.
Short Hold	
Short Hold	The "short hold" operating mode is turned on for the PPP connection. The following entry is only possible when short-hold mode is enabled.

Parameters	Description
Short Hold Time (sec)	Length of time without data transmissions after which the PPP connection should be cleared. The short hold timer is only triggered by outgoing packets. Value range, default value: 10 - 9999, 60
Authentication	
PPP Authentication	PPP authentication is enabled. The setting must be made in accordance with the specifications of the ISP.
PPP User Name	Freely selectable user name to be used for authentication via PAP or CHAP.
PAP Authentication Mode	Activation and type of PAP authentication for the PPP connection: Not used, PAP Client, PAP Host.
PAP Password	Password for PAP authentication.
CHAP Authentication Mode	Activation and type of CHAP authentication for the PPP connection: Not used, CHAP Client, CHAP Host, CHAP Client and Host.
CHAP Password	Password for CHAP authentication.
Data Compression	
DEFLATE Data Compression	For the compression of PPP data packets with the compression algorithm DEFLATE.
COMPRESS Data Compression	For the compression of PPP data packets with the compression algorithm COMPRESS.
Address Translation	
NAT	NAT (Network Address Translation) is turned on. The following protocols are supported: TCP, UDP and ICMP (only in passive mode).
Address Mapping	will be dropped.
Router Settings	
Full-Time Circuit	Depending on the tariff model, the full-time circuit (permanent connection) to the ISP can be enabled or disabled. The full-time circuit should be disabled for a time-based tariff model and enabled for a flat rate tariff model.
Short Hold Time (sec)	If Full-Time Circuit is disabled (time-based tariff model), enter the duration of inactivity after which the connection is to be dropped (e.g., 60 seconds). Value range, default value: 10 - 9999, 60
Forced Disconnect at (hour:min)	If Full-Time Circuit is enabled (flat-rate tariff model), enter the time at which the Internet connection is to be deactivated (e.g., 04:59).
Connection Time	Displays the elapsed connection time in days-hours-minutes-seconds.
QoS Parameters of Interface	
Bandwidth for Downloads	Value of the full download bandwidth in Kbps provided by the ISP.
Bandwidth for Uploads	Value of the full upload bandwidth in Kbps provided by the ISP.

Parameters	Description
Bandwidth Control for Voice Connections	Bandwidth control prevents the transmission rates available from being overbooked with voice connections within a multi-link connection. In other words, when header compression is active, a maximum of 5 voice connections are permitted over a B channel. This field enables bandwidth control for voice connections. Only voice connections with routes configured in the voice gateway are considered here.
Bandwidth Used for Voice/ Fax (%)	Percentage of bandwidth available for voice/fax connections. Value range, default value: 0 - 100, 80

Parameter Description of Tabs:

- **Edit ACD**

Parameters	Description
Connection Time	Displays the elapsed connection time in days-hours-minutes-seconds.
Force Reconnect at	Time at which the connection is to be cleared and reestablished.
Enable ACD	Enable automatic cleardown to pre-empt disconnection by the ISP at an inopportune time.

28.3.3.3 Network Interfaces > Mainboard > LAN 2

Parameter Description of Tabs::

- **Edit LAN 2 Interface**

Parameters	Description
Internet access via an external Router	Access to the Internet occurs via an external router.
Interface Is Active	The LAN interface is enabled.
IP address	IP address of the communication system.
Subnet Mask:	Subnet mask of the LAN segment in which the communication system is located.
MAC Address	Displays the MAC address of the communication system.
Ethernet Link Mode	LAN interface mode.
Ethernet Link Mode: Auto	Automatic switching between 100 and 1000 Mbps full duplex mode. In this mode, you can enable the power management. After migration to V2R3 or later Apply on top must be pressed for the desired ethernet link through the network interface page in order the value to be se to Auto. Otherwise, the systems must be set to Auto or 100 before migration.
Ethernet Link Mode: 100HDX	100 Mbps, full duplex. Power management cannot be enabled in this mode.

Parameters	Description
Ethernet Link Mode: 100FDX	100 Mbps, full duplex. Power management cannot be enabled in this mode.
Ethernet Link Mode: 1000FDX	1000 Mbps, full duplex. Power management cannot be enabled in this mode.
IEEE802.1p/q Tagging	If this check box is selected, a "type of service" is included in the Ethernet packets (Layer 2) for prioritization purposes The option is deactivated by default.
IEEE802.1p/q VLAN ID	Enter the VLAN's ID number only if the used switch has problems with the default value "0".
Layer 2 QoS Class	
Signaling Data	Priority class for the connection setup. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 3
Fax/Modem Payload	Priority class for the fax and modem data of the IP connection. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 5
Network Control	Priority class for the network control data (transfer of SNMP traps, for example). 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 0
Voice Payload	Priority class for the voice data. 0 = lowest priority / 7 = highest priority. Value range, default value: 0 - 7, 5

28.3.3.4 Network Interfaces > Mainboard > LAN 3 (Admin)

Parameter Description of Tabs::

- **Edit LAN 3 Interface**

Parameters	Description
Interface Is Active	The LAN interface is enabled.
Automatic Address Configuration (via DHCP)	An external DHCP server assigns an IP address to the communication system.
Accept IP Address of the Default Router	The external DHCP server communicates the IP address of the default router (e.g., the Internet router) to the communication system.
Accept IP Address of the DNS Server	The external DHCP server communicates the IP address of the DNS server to the communication system.
Accept IP Address of the SNTP Server	The external DHCP server communicates the IP address of the SNTP server to the communication system.
IP address	IP address of the LAN interface.
Subnet Mask:	Netmask of the LAN segment.

Parameters	Description
MAC Address	Displays the MAC address of the LAN interface.
Ethernet Link Mode	LAN interface mode.
Ethernet Link Mode: Auto	Automatic switching between 100 and 1000 Mbps full duplex mode.
Ethernet Link Mode: 100HDX	100 Mbps, full duplex.
Ethernet Link Mode: 100FDX	100 Mbps, full duplex.
Ethernet Link Mode: 1000FDX	1000 Mbps, full duplex.

28.3.3.5 Network Interfaces > Mainboard > FTP Server

Parameter Description of Tabs::

- **Edit FTP Server Parameters**

Parameters	Description
Enable FTP Server	If this check box is selected, the internal FTP server is released.
Download User 'Phone'	
Name	Name for the access of IP phones to the FTP server to download the latest software updates. The name cannot be changed.
New password	Password for the access of IP phones to the FTP server. If the predefined password is changed, the password must also be changed at the IP phones.
Confirm Password	Password for the access of IP phones to the FTP server.
Download User 'ftpadmin'	
Name	Name of administrator access to the FTP server. The name cannot be changed.
New password	Password for administrator access to the FTP server.
Confirm Password	Password for administrator access to the FTP server.

28.3.3.6 Network Interfaces > Mainboard > DHCP Mode

Parameter Description of Tabs::

- **Edit DHCP Mode**

Parameters	Description
No DHCP	Enabling this radio button disables the internal DHCP server.
DHCP Server	Enabling this radio button enables the internal DHCP server.

Parameters	Description
DHCP Relay Agent	Enabling this radio button causes the communication system to act as a DHCP relay agent. The DHCP requests of the IP stations are forwarded from the communication system to the actual DHCP server. The DHCP server and the IP stations do not have to be in the same network segment.

28.3.3.7 Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Global Parameters

The network-specific data is transmitted from the DHCP server to the IP stations.

Parameter Description of Tabs::

- **Edit Global Parameters**

Parameters	Description
Enable DHCP Server	Indicates that the internal DHCP server is enabled and that its global parameters can be configured. Cannot be changed.
Mitel/Unify Devices Only	Indicates that the internal DHCP server is accepting requests only from Mitel and Unify phone devices. If the client receives more than one answers, for example from the OpenScape Business DHCP server and from another server in the network, it will prefer the answer received from OpenScape Business, if using compatible devices: • OpenScape DeskPhone CP x00 with software release V1R8.4.0 (HFA) / V1R11.6.0 (SIP) or higher • OpenScape DeskPhone CP x10 with software release V2R0.18.0 (HFA or SIP) or higher • Mitel MiVoice 69xx / 68xx (SIP)
Subnet Mask:	The subnet mask defines the size of the subnet. Example: `255.255.255.0`.
Broadcast Address	With the broadcast address, all IP stations of a network or subnet can be addressed by the DHCP server (optional). Example: `0.0.0.0`.
Default Gateway	
Gateway 1	IP address under which the default gateway can be reached. If an Internet router is used in the network, the Internet router is the default gateway. Example: `192.168.1.1`. If the communication system is directly connected to an Internet modem, the communication system is the default gateway. Example: `192.168.1.2`.
Gateway 2	IP address under which a second default gateway (router) can be reached (optional).
Gateway 3	IP address under which a third default gateway (router) can be reached (optional).
DNS Server	

Parameters	Description
Domain Name	Domain name of the internal network, max. 80 characters, e.g., `mynet.home` (optional).
Server 1	IP address under which the DNS server can be reached. If the communication system is directly connected to an Internet modem, the default value `0.0.0.0` must not be changed. The communication system uses it to automatically connect to a DNS server from the Internet. An external DNS server can also be entered. Example: the DNS server of the Internet router (`192.168.1.1)` or a DNS server from the Internet (`google-public-dns-a.google.com`).
Server 2	IP address under which a second DNS server can be reached (optional).
Server 3	IP address under which a third DNS server can be reached (optional).
Lease time in hours (0 infinite)	Maximum validity period in hours, 0 = infinite lifetime (default: 1 hour).
Enable Dynamic DNS Update	If this check box is enabled, the DNS server may be dynamically updated. Default: not enabled. **NOTICE:** If Dynamic DNS Update option is enabled, it is mandatory to configure **Domain Name** in IP Address Pool respective Domain name field.
Use Internal DLI	If this check box is selected, the internal DLI is used. If is check box is cleared, the parameters for an external DLS server appear. Default: enabled.
External DLS Server	
IP address	IP address under which the external DLS server can be reached.
Port	Port through which the external DLS server can be reached.

28.3.3.8 Network Interfaces > Mainboard > DHCP Mode > DHCP Server > IP Address Pools

Parameter Description of Tabs::

- **Display IP Address Pools**
- **Add IP Address Pool**
- **Edit IP Address Pool**
- **Delete IP Address Pool**

Parameters	Description
Subnet address	The subnet address defines the maximum IP address range. Example: `192.168.1.0`.
Subnet Mask:	The subnet mask defines the size of the subnet. Default setting: `255.255.255.0`.

Parameters	Description
address range	
Address range 1	Lower and upper limits of the IP address range of the subnet. Example: from `192.168.1.50` to `192.168.1.254`.
Address range 2	Lower and upper limits of a second IP address range within the same subnet (optional).
Address range 3	Lower and upper limits of a third IP address range within the same subnet (optional).
Default Gateway	
Gateway 1	IP address under which the default gateway can be reached. If an Internet router is used in the network, the Internet router is the default gateway. Example: `192.168.1.1`. If the communication system is directly connected to an Internet modem, the communication system is the default gateway. Example: `192.168.1.2`.
Gateway 2	IP address under which a second default gateway (router) can be reached (optional).
Gateway 3	IP address under which a third default gateway (router) can be reached (optional).
Broadcast Address	With the broadcast address, all IP stations of a network or subnet can be addressed by the DHCP server (optional). Default: `0.0.0.0`.
Domain Name	Domain name of the internal network, max. 80 characters, e.g., `mynet.home` (optional).
DNS Server	
Server 1	IP address under which the DNS server can be reached. If the communication system is directly connected to an Internet modem, the default value `0.0.0.0` must not be changed. The communication system uses it to automatically connect to a DNS server from the Internet. An external DNS server can also be entered. Example: the DNS server of the Internet router (`192.168.1.1)` or a DNS server from the Internet (`google-public-dns-a.google.com`).
Server 2	IP address under which a second DNS server can be reached (optional).
Server 3	IP address under which a third DNS server can be reached (optional).
Enhanced Security	
Relay Option	A hexadecimal number configured by the administrator for extra security. The value of this field is empty by default, and this option will not be taken into account if not configured.
Lease time in hours (0 infinite)	Maximum validity period in hours, 0 = infinite lifetime (default: 1 hour).

28.3.3.9 Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Static IP Addresses

Parameter Description of Tabs::

- **Display Static IP Address**
- **Add Static IP Address**
- **Edit Static IP Address**
- **Delete Static IP Address**

Parameters	Description
Hostname	Name or description of the IP station (e.g., PC or server) that is to receive a fixed IP address. Example: `Print Server`.
IP address	Desired fixed IP address. Example: `192.168.1.10`.
Client Identifier	MAC address of the IP station ex. Mitel SIP-DECT RFP device.
Subnet Mask:	Netmask of the subnet. Example: `255.255.255.0`.
Default Gateway	
Gateway 1	IP address under which the default gateway can be reached. If an Internet router is used in the network, the Internet router is the default gateway. Example: `192.168.1.1`. If the communication system is directly connected to an Internet modem, the communication system is the default gateway. Example: `192.168.1.2`.
Default Gateway 1	IP address under which a second default gateway (router) can be reached (optional).
Default Gateway 1	IP address under which a third default gateway (router) can be reached (optional).
Broadcast Address	With the broadcast address, all IP stations of a network or subnet can be addressed by the DHCP server (optional). Example: `0.0.0.0`.
Domain Name	Domain name of the internal network, max. 80 characters, e.g., `mynet.home` (optional).
DNS Server	
Server 1	IP address under which the DNS server can be reached. If the communication system is directly connected to an Internet modem, the default value `0.0.0.0` must not be changed. The communication system uses it to automatically connect to a DNS server from the Internet. An external DNS server can also be entered. Example: the DNS server of the Internet router (`192.168.1.1)` or a DNS server from the Internet (`google-public-dns-a.google.com`).
Server 2	IP address under which a second DNS server can be reached (optional).
Server 3	IP address under which a third DNS server can be reached (optional).
Enhanced Security	

Parameters	Description
Relay Option	A hexadecimal number configured by the administrator for extra security.
Lease time in hours (0 infinite)	Maximum validity period in hours, 0 = infinite lifetime (default: 1 hour).

28.3.3.10 Network Interfaces > Mainboard > DHCP Mode > DHCP Server > Last active Leases

The IP address assigned by a DHCP server remains valid for an IP station until the "lease period" expires, even if the IP station is turned off during that time. The last active assignments are displayed here.

Parameter Description of Tabs::

- **Display Lease**
- **Delete Lease**

Parameters	Description
IP address	IP address assigned to the IP station by the DHCP server.
MAC Address	MAC address of the IP station to which an IP address was assigned.
Client ID	Client ID of the IP station. If the client ID is not available, the MAC address of the IP station is displayed.
Hostname	Name or call number of the IP station to which an IP address was assigned.
Start of lease	Start time of the assignment. The IP station is assigned an IP address as of this point in time.
End of lease	Ending time of the assignment. After this period, the IP station needs to send a new request for an IP address.

28.3.3.11 Network Interfaces > Mainboard > DHCP Mode > DHCP Server > All Leases

The IP address assigned by a DHCP server remains valid for an IP station until the "lease period" expires, even if the IP station is turned off during that time. All assignments are displayed here.

Parameter Description of Tabs::

- **Display Lease**
- **Delete Lease**

Parameters	Description
IP address	IP address assigned to the IP station by the DHCP server.
MAC Address	MAC address of the IP station to which an IP address was assigned.
Client ID	Client ID of the IP station. If the client ID is not available, the MAC address of the IP station is displayed.

Parameters	Description
Hostname	Name or call number of the IP station to which an IP address was assigned.
Start of lease	Start time of the assignment. The IP station is assigned an IP address as of this point in time.
End of lease	Ending time of the assignment. After this period, the IP station needs to send a new request for an IP address.

28.3.3.12 Network Interfaces > Application Board > Host Name

Parameter Description of Tabs::

- **Editing the Host Name**

Parameters	Description
Host Name	Host name of the Application Board - freely selectable. Example: `applboard` If the name and IP address of the Application Board are stored on a DNS server, name resolution can occur. The name of the Application Board is composed of the host name and the domain name. Example: `applboard.mynet.home`

28.3.3.13 Network Interfaces > Application Board > LAN 1

Parameter Description of Tabs::

- **Edit Lan 1 Interface**

Parameters	Description
Interface Is Active	If this check box is selected, the LAN 1 interface of the Application Board is active.
Automatic Address Configuration (via DHCP)	If this check box is selected, the IP address and subnet mask are automatically assigned by the DHCP server for the LAN 1 interface. In addition, it is also possible to select whether further network-specific parameters are to be transferred from the DHCP server.
Accept IP Address of the Default Router	If this check box is selected, the IP address of the default router is taken over by the DHCP server.
Accept IP Address of the DNS Server	If this check box is selected, the IP address of the DNS server is taken over by the DHCP server.
Accept IP Address of the SNTP Server	If this check box is selected, the IP address of the SNTP server is taken over by the DHCP server.
IP address	IP address under which the Application Board can be reached.
Subnet Mask:	Subnet mask under which the Application Board can be reached.
MAC Address	MAC address of the Application Board (not editable).

Parameters	Description
Ethernet Link Mode	Mode of the LAN 1 interface.
Ethernet Link Mode: Auto	Automatic switching between 100 and 1000 Mbps full duplex mode. In this mode, you can enable the power management.
Ethernet Link Mode: 100HDX	100 Mbps, full duplex. Power management cannot be enabled in this mode.
Ethernet Link Mode: 100FDX	100 Mbps, full duplex. Power management cannot be enabled in this mode.
Ethernet Link Mode: 1000FDX	1000 Mbps, full duplex. Power management cannot be enabled in this mode.

28.3.3.14 Network Interfaces > Application Board > LAN 2

Parameter Description of Tabs:

- **Edit Lan 2 Interface**

Parameters	Description
Interface Is Active	If this check box is selected, the LAN 2 interface of the Application Board is active.
IP address	IP address under which the Application Board can be reached.
Subnet Mask:	Subnet mask under which the Application Board can be reached.
MAC Address	MAC address of the Application Board (not editable).
Max. Data Packet Size (Bytes)	Maximum packet length in bytes applicable for the IP protocol. Values between 576 and 1500 are permitted.
Ethernet Link Mode	Mode of the LAN 2 interface.
Ethernet Link Mode: Auto	Full duplex mode. In this mode, you can enable the power management.
Ethernet Link Mode: 100HDX	100 Mbps full duplex. Power management cannot be enabled in this mode.
Ethernet Link Mode: 100FDX	100 Mbps, full duplex. Power management cannot be enabled in this mode.
Ethernet Link Mode: 1000FDX	1000 Mbps, full duplex. Power management cannot be enabled in this mode.
IEEE802.1p/q Tagging	If this check box is selected, the Ethernet format used by the Application Board is set. The option is deactivated by default.
IEEE802.1p/q VLAN ID	Enter a value that differs from the default value "0" as the VLAN's ID number if the switch used has problems with the default value "0".
Layer 2 QoS Class	
Signaling data	Priority class for the connection setup. 0 = lowest priority / 7 = highest priority.

Parameters	Description
Fax/Modem Payload	Priority class for the fax and modem data of the IP connection. 0 = lowest priority / 7 = highest priority.
Network Control	Priority class for the network control data (transfer of SNMP traps, for example). 0 = lowest priority / 7 = highest priority.
Voice Payload	Priority class for the voice data of the IP connection. 0 = lowest priority / 7 = highest priority.

28.3.4 Routing

Routing tables are managed under **Routing**. In small networks, a routing table can be set up manually on every router by the administrator. In larger networks, this task is automated with the help of a protocol that distributes routing information in the network.

28.3.4.1 Routing > IP Routing > Mainboard > Static Routes

The communication system supports static routes only. Static routes connect two IP devices with each other. They are created manually.

Depending on the application, it may be necessary to set a different routes for the system (mainboard) and the UC Booster Card (Application Board).

Parameter Description of Tabs::

- **Display Static Route Table**
- **Add Static Route**
- **Edit Static Route**
- **Delete Static Route**

Parameters	Description
Route Index:	The route index is automatically assigned and only displayed for information purposes. It cannot be modified.
Route Name:	Name or description of the static route; freely selectable.
Destination Network/Host:	IP address of the destination network.
Subnet Mask:	Subnet mask of the destination network.
Route Gateway:	IP address of the next router on this route or IP address of the local or remote interface of a PSTN peer.

28.3.4.2 Routing > IP Routing > Mainboard > Default Router

Depending on the application, it may be necessary to set a different default routing for the system (mainboard) and the UC Booster Card (Application Board).

Parameter Description of Tabs::

- **Edit Default Router**

Parameters	Description
Default Routing via	Enable or disable IP routing via a default router.
No interface	Disable IP routing via a default router.
LAN	Enable IP routing via a default router.
IP Address of Default Router	IP address of the default router, provided **LAN** is selected as the interface in the **Default Routing via** field. Example: IP address of the Internet router, `192.168.1.1`.

28.3.4.3 Routing > IP Routing > Mainboard > DNS Server

You can display, and where applicable, edit the IP address of the DNS server. The setting is necessary for trunking with dynamic IP addresses.

Parameter Description of Tabs::

- **Edit DNS Settings**

Parameters	Description
IP Address of DNS Server	IP address under which the DNS server can be reached. If the communication system is directly connected to an Internet modem, the default value `0.0.0.0` must not be changed. The communication system uses it to automatically connect to a DNS server from the Internet. An external DNS server can also be entered. Example: the DNS server of the Internet router (`192.168.1.1)` or a DNS server from the Internet (`google-public-dns-a.google.com`). In case of an OpenScape Business S system, a system reboot is necessary in order the changes to be applicable.

28.3.4.4 Routing > IP Routing > Application Board > Static Routes

Depending on the application, it may be necessary to set a different routes for the system (mainboard) and the UC Booster Card (Application Board).

Parameter Description of Tabs:

- **Display Static Route Table**
- **Add Static Route**
- **Edit Static Route**
- **Delete Static Route**

Parameters	Description
Route Index:	The route index is automatically assigned and only displayed for information purposes. It cannot be modified.
Route Name:	Name or description of the static route; freely selectable (optional) Value range: max. 35 characters
Destination Network/Host:	IP address of the destination network.
Subnet Mask:	Subnet mask of the destination network.
Route Gateway:	IP address of the next router on this route or IP address of the local or remote interface of a PSTN peer.

28.3.4.5 Routing > IP Routing > Application Board > Default Router

Depending on the application, it may be necessary to set a different default routing for the system (mainboard) and the UC Booster Card (Application Board).

Parameter Description of Tabs::

- **Change Default Router**

Parameters	Description
Default Routing via	Enable or disable IP routing via a default router.
No interface	Disable IP routing via a default router.
LAN	Enable IP routing via a default router.
IP Address of Default Router	IP address of the default router, provided LAN is selected as the interface in the "Default Routing via" field.

28.3.4.6 Routing > NAT

NAT rules for network address translation can be displayed, added, edited and deleted. The NAT Table Editor allows you to edit all existing and new NAT entries at once for network address translation.

Parameter Description of Tabs::

- **Add NAT**
- **NAT Table Editor**

Parameters	Description
NAT Rule Active	
Description	
Local IP Address	Local destination address on the LAN.
Local port	Enter the port number of the active LAN protocol.

Parameters	Description
Global Port	Port number of the active protocol.
Protocol	Transport protocol to be used. The set transport protocol applies both for local and global addresses.
Protocol: **TCP**	TCP (Transmission Control Protocol) TCP is a reliable, connection-oriented protocol for the transmission of IP packets. Before transfer starts, a virtual channel is set up between the two terminal points. Data can be transmitted in both directions on this channel. TCP is mainly used in the WorldWideWeb and in e-mail and peer-to-peer networks. It is also used for call signaling in IP telephony because it can detect and automatically rectify data losses during transmission.
Protocol: **UDP**	UDP (User Datagram Protocol) UDP is a reliable, connectionless protocol for the transmission of IP packets. In contrast to TCP/peer scenarios, a virtual channel is not set up before transfer starts so that the PCs can start transferring data without delay. In UDP, the port number of the service that should receive the data is included when addressing voice packets. It is mainly used in the DNS sector and for voice transmission in IP telephony. However, since a connectionless protocol does not check if the peer actually received the data, this option can result in voice transfer losses.

28.3.4.7 Routing > PSTN

These parameters are used to set up an IP remote connection (dial-up) via the traditional telephone network.

Parameter Description of Tabs::

- **Edit Global PSTN Data**

Parameters	Description
Router Call Number(Internal Call Number)	Used to select the DID number of the system. All applications that use the router function can be reached from an external location via this DID number. External routing partners that do not transfer a station number must each use different call numbers. These station numbers are configured as MSNs.
Redialing	
Number of Redial Attempts	Number of redial attempts that should be made by the system to set up a connection Value range: 0 to 255
Pause between Redial Attempts (sec)	Interval between redial attempts in seconds. Value range: 1 - 1,.000
Scripting	

Parameters	Description
Identification of User 1 for Scripting	First part of account credentials to log in at Internet providers. The Internet provider requires host, user identification and password entries, for example, Host=ERT005, User=KJUMBERT, Password=123456. The entries are therefore as follows: Identification of User 1 for Scripting: HOST:ERT005 - Identification of User 2 for Scripting: USER:KJUMBERT - New Password for Scripting: PASSWORD:123456.
Identification of User 2 for Scripting	Second part of account credentials to log in at Internet providers.
New Password for Scripting	Password to log in at Internet Providers.

28.3.4.8 Routing > PSTN > PPP Log

Parameter Description of Tabs:

- **Load via HTTP**

Parameters	Description
Load	The PPP log file can be loaded via HTTP. Depending on your browser settings, you will be prompted to select whether the downloaded log file should be saved or opened in the default editor.

28.3.4.9 Routing > PSTN > PSTN Partner

Parameter Description of Tabs::

- **Add PSTN Peer**
- **Display PSTN Peer**
- **Edit PSTN Peer**

Parameters	Description
Peer Name	PSTN Peer Name. The following PSTN peers are available: • Default PSTN - not configurable • PSTN Peer 1: default for CLA, reconfigurable function • PSTN Peer 2: default for ISDN, reconfigurable function • PSTN Peer 3: name and function freely configurable • PSTN Peer 4: name and function freely configurable Value range: 1 to 14 characters
PSTN Connection Type	Setup of the PSTN Connection: (Default selection: Enabled).
PSTN Connection Type: Not configured	PSTN peers can be preconfigured. However, this setting prevents a connection being set up over this PSTN peer.
PSTN Connection Type: Active	PSTN peer is enabled. This setting allows a connection to be set up via this PSTN peer.

Parameters	Description
PSTN Connection Type: DSL Fallback	Use of the DSL access for the PSTN connection (the default router is the DSL access)
IP parameters	
IP Address of PSTN Peer	IP address of the host PC on the peer side, to which the PSTN connection is established.
IP Address of Local PSTN Interface	IP address of the local communication system, which is used for the PSTN connection.
IP Address Negotiation	Negotiation of the IP address between the connection partners when setting up the connection.
IP Address Negotiation: configured IP address	Only the configured IP address of the PSTN peer is accepted.
IP Address Negotiation: accept any IP address	No IP address negotiation
IP Address Negotiation: request new IP address	The IP address is negotiated
General PPP Parameters	
Default Router	The PSTN peer set up here should not only be preconfigured, but also used as a routing destination. There can only be one default router. This is either the DSL access or the PSTN peer set up here.
Internet Access with DNS Request	The access is to be used for Internet access. Only one Internet access per system may be activated (either a PSTN partner or a DSL connection).
Service Entry	The Call no. test function should be disabled when calling the MSN of the PSTN peer. The Service Entry function can only be activated if the PSTN peer has an MSN number and a PAP or CHAP authentication has been activated.
MSN/DID Number(Internal Call Number)	Configuration of the MSN number. A station number transferred by the partner must be configured, as otherwise the call is rejected. If, on the other hand, the partner has configured call numbers but does not transfer any, a connection will be set up anyway.
B channels	Number of used B channels. Value range: 1 or 2
Callback	A call is rejected, and the peer is then called back immediately. This prevents unauthorized peers from dialing in. The calling station must use the ISDN connection's D channel to transfer the station number and must permit dial-in via the system. This station number must be configured for the outgoing direction at the PSTN peer. If callback is enabled, only outgoing connections from this peer are accepted. A connection cannot be set up if the peer is also a gateway and if callback is also enabled for this connection, since neither of the peers accepts an incoming connection setup. In the case of such a faulty configuration where only "callback without redial" is enabled, this can be detected, and a continuous connection setup can be suppressed. However, the problem is not detected if redial is enabled.
V.34 Peer	Accept a V.34 Peer (e.g., a modem).

Parameters	Description
Automatic PPP Reconnection	The PPP connection is automatically reestablished after a connection cleardown (for example, in the case of ISP access with flat rate and a forced disconnect after 24 hours).
Send LCP Echo Request	An LCP echo request is sent. This function is used to check if the connection is still active.
Short Hold	
Short Hold	The "short hold" operating mode is turned on for the PPP connection. The following entries are only possible when short-hold mode is active.
Short Hold Time (sec)	Length of time without data transmissions after which the PPP connection should be cleared. The Short Hold Timer is only triggered by outgoing packets. Value range: 10 to 9999
Short Hold Charge Pulse Analysis	Optimization of the short-hold mode, taking the charge pulse into account. Charge pulse analysis is performed for calls over PPP (evaluation of facility messages with AoC info elements). If the Internet service provider does not supply call charge information, then the default timeout value is set to 0 seconds.
Authentication	
PPP Authentication	PPP authentication is enabled.
PPP User Name	Freely selectable user name to be used for authentication via PAP or CHAP.
PAP Authentication Mode	Activation and type of PAP authentication for the PPP connection: Not used, PAP Client, PAP Host.
PAP Password	Password for PAP authentication.
CHAP Authentication Mode	Activation and type of CHAP authentication for the PPP connection: Not used, CHAP Client, CHAP Host, CHAP Client and Host.
CHAP Password	Password for CHAP authentication.
Header Compression	
IP Header Compression	The compression of the IP/TCP or IP/UDP/RTP header is enabled. Header compression improves data transmission in Voice-over-PPP scenarios. All voice packets with UPD port numbers in the set range are compressed.
Data Compression	
DEFLATE Data Compression	Compression using the DEFLATE algorithm
COMPRESS Data Compression	Compression with the COMPRESS algorithm
Address Translation	
NAT	NAT (Network Address Translation) is turned on. The following protocols are supported: TCP, UDP and ICMP (only in passive mode).
Address Mapping	Address mapping is enabled.

Parameters	Description
QoS Parameters of Interface	
Bandwidth Control for Voice Connections	Bandwidth control prevents the transmission rates available from being overbooked with voice connections within a multi-link connection. In other words, when header compression is active, a maximum of 5 voice connections (G.729 / 60 msec or G.723/60 msec) are permitted over a B channel. This field enables bandwidth control for voice connections. Only voice connections with routes configured in the voice gateway are considered here.
Bandwidth Used for Voice/ Fax (%)	Percentage of bandwidth available for voice/fax connections. Value range, default value: 0 - 95, 80

Parameter Description of Tabs::

- **Reset to Factory Default**

Parameters	Description
Apply	The values for the selected PSTN partners are reset to the factory default values.

Parameter Description of Tabs::

- **Add Call Number**
- **Change station number**
- **Delete Call Number**

Parameters	Description
Call number	The call number at which the PSTN peer can be reached. It must be unique within the entire configuration and can comprise up to 22 decimal digits (0 to 9). Hyphens are permitted. Up to five call numbers can be configured for each PSTN peer. A station number is checked as it is being transferred, and calls are only accepted if a PSTN peer is assigned appropriate call authorization for the incoming station number.
Call direc.	The connection occurs under the phone number entered above.
Call direc.: Blocked	The number cannot be used.
Call direc. : incoming	The peer may make calls but may not be called.
Call Direction: outgoing	The peer may be called but may not make calls.
Call direc. : Incoming and Outgoing	The peer may be called and can also make calls.
Delete	The dialed station number will be deleted.

28.3.5 LCR

The Least Cost Routing features such as classes of service, dial plans, routing tables, and dial rules are grouped under **LCR**.

28.3.5.1 LCR > LCR flags

Parameter Description of the Tab:

- **Edit LCR Flags**

Parameters	Description
LCR Flags	
Activate LCR	LCR is activated and thus enables least cost routing.
Reset LCR data	
Delete the configured LCR data and initialize the LCR with default data	If this radio button is selected, the configured LCR entries (dial plans, routing tables, dial rules) are deleted and replaced by the default entries.

INFO: An invalid configuration in the LCR could potentially prevent or restrict outgoing connections.

Related concepts

Station Data on page 153

28.3.5.2 LCR > Classes Of Service

Parameter Description of the Tab:

- **Edit LCR Classes of Service**

Parameters	Description
Index	Hierarchical index list
Phone number	Station number
Name	Name of the station
Access groups	Every subscriber is assigned to an LCR class of service (COS) group. By default, all subscribers are entered with the maximum LCR Class of Service (15) Value range: 1 to 15

INFO: A subscriber can only seize a route if his or her COS is greater than or equal to the LCR COS in the routing table.

28.3.5.3 LCR > Dial Plan

Parameter Description of Tabs::

- **Change Dial Plan**

- **Display Dial Plan**

Parameters	Description
Dial Plan	The dial plan is searched for patterns that match the dialed digits. The result is used as a criterion for selecting the route table. At the same time, the system checks if the subscriber's class of service matches for this route. For external connections, each call number including the code (up to a maximum of 24 characters incl. field separators) is checked in the dial plan. The dial plan then determines a route table for the station; the station is assigned this table for the connection setup. Up to 16 routes are created via a single route table. The Dialing rules table defines how the digits selected by the station are converted and dialed by the communication system.
Name	The Name column can be used to assign a name to each profile, e.g., local call, long-distance call, international, etc. Depending on the version of the communication system, the Name column may or may not be displayed. A meaningful name should be selected when assigning names. Multiple instances of the same name may be used. Appropriate names are automatically assigned via the Dial Rule wizard.
Dialed digits	Using this scheme, the call number is evaluated in order to branch to the appropriate route table. The field delimiters C and - as well as the placeholders X, N and Z can be used. Fixed digits 0...9 - Field delimiters (evaluation through the dial rule); X - placeholder for a digit from 0...9; N - placeholder for a digit from 2..9; Z - placeholder for one or more digits until end of dialing; C - simulated dial tone (can be entered a maximum of 3 times)
Route table	The Route table column is used to specify which route table is to be used for the profile. The arrow links to the definition of the respective route table. Value range: 1 to 254, of which 1 to 15 preset
Acc. code	The checkbox for this column is selected/cleared to determine whether or not an account code entry is mandatory after the seizure code (in the U.S.: after end-of-dialing). When the checkbox is cleared, the account code is not required until the dial plan has been dialed completely if it has been configured for the route.
Toll restriction	When selected, the dialed digits are subject to toll restriction (class of service). This applies to networking, as well as to standalone communication systems. With this, individual call numbers can be removed from the toll restriction. If the toll restriction should be applied, the known rules for Allowed/Denied Lists apply.
Emergency	If a number that was configured as an emergency number (emergency column checkbox selected) is dialed, and no free line is available, then a line that is being used for a non-emergency number (emergency column checkbox cleared) is disconnected and then made available automatically for the emergency number.

28.3.5.4 LCR > Routing Table

Parameter Description of Tabs:

- **Change Routing Table**

Parameters	Description
Route tables	Call numbers defined in the dial plan are assigned an action (choice) here via the route tables. Value range: 254 route tables
Index	The route table is searched from top to bottom in hierarchical order. The system checks to determine whether the route is free and the station has the requisite LCR class of service. If this is the case, dialing occurs in accordance the outdial rule and schedule entered in the route table. Value range: 1 to 16
Dedicated Route	The fixed route that was assigned to the subscriber (e.g., via the route assignment of the multisite management) is used.
Route	For details on the route to be assigned, see "Trunks/Routing > Routes" Default value: Route name configured in the system
Dial Rule	LCR outdial rules can be used to convert the phone numbers entered into random new digit strings for additional processing. Access to different carriers is enabled via digit translation. Definition under "Dial Rule". Value range: 254 dial rules
min. COS	COS describes the minimum LCR class-of-service needed by a station in order to use the associated route. It is thus possible to stipulate, for example, that one station is only permitted to place calls via a specific carrier or during certain times, while other stations have the option of using alternative routes. The value for the maximum class of service is 15. Value range: 1 to 15
Warning	If the first route selection in the route table is busy, the LCR function advances to the next (possibly more expensive) route configured in the route group table. The system can notify the user of this with an audible signal, an optical signal, or both. Value range: None, Tone, Display, Display + Tone
Dedicated Gateway	This parameter defines the way in which the destination partner node is identified in an IP internetwork. Value range: No, Forced, Multi-location
Dedicated Gateway: **No**	The partner node is identified by the destination call number.
Dedicated Gateway: **Forced**	Routed is forced via the gateway that is defined by its node ID in the **GW Node ID** column.
Dedicated Gateway: **Multi-location**	Caller-based determination of the partner node: Routing occurs via the gateway that was assigned to the respective caller via the Multigateway wizard or in the **Stations** > **Edit workpoint client data** > **Secondary system ID** input mask. For callers without a related entry, routing occurs via the gateway that is defined by its node ID in the **GW node ID** column (default).
GW Node ID	Specifies the gateway node ID for the **Forced** or **Multi-location** options of the **Dedicated Gateway** parameter.
Buttons	

Parameters	Description
Blue arrow in the **Dial Rule** column	Displays the page with the **Dial Rule** parameters.

28.3.5.5 LCR > Dial Rule

Parameter Description of the Tab:

- **Edit Outdial Rule**

Parameters	Description
	LCR outdial rules can be used to convert the phone numbers entered into random new digit strings for additional processing. Access to different carriers is enabled via digit translation. The dial rule used is defined by the route table entry.
Rule Name	Freely definable name of the dial rule; some dial rules are predefined Value range: max. 16 characters
Dial rule format	Program for the digits to be dialed. The individual program steps are processed from left to right. The characters for the program code represent the following functions:
A	Repeat remaining fields (transmit). The letter "A" causes all subsequent digit fields to be transmitted. The point of reference is the last field delimiter in the field of dialed digits in the dial plan. If "A" is entered without an explicit reference, it designates all digits after the acces code, i.e., "A" is then equivalent to "E2A"
B	It is used for the multi-gateway network when a station number of type TON (Type Of Number) that was called from outside is "unknown" and must be routed to the multi-gateway node. To ensure that this station number is unique, it is extended to national or international in accordance with the TON in the LCR. This is required when the DID numbers are not unique and need to be configured in the national or international format.
D (n)	Dial digit sequence (1 to 25 digits). "D" may occur multiple times and at any position in the string.
E (n)	Transmit field contents (1 to 10). "E" may occur multiple times and at any position in the string. "E" can also appear in any order with relation to (n). A specific field can be addressed multiple times, including in sequence. With the exception of "E1" (access code), this letter may be surrounded by any other parameters. With digit-by-digit dialing (as opposed to en-bloc dialing), the last element in the outdial rule must not be E(n), but E(n)A.
M (n)	Authorization code (1 to 16). This letter must not be in the final position.
P (n)	P (n) can occur more than once in the string and can be placed in any position. P (n) can be surrounded by any other parameters.(1 to 60 times the system-wide pause unit).

Parameters	Description
S	Switch, changes signaling methods from DP to DTMF (with CONNECT, PROGRESS or CALL PROC with PI). The letter "S" may occur in the string only once and must not be in the final position. The "C" parameter cannot be used after "S".
C	Carrier "C" can be inserted in the string only once. The subsequent characters are transmitted without a dial pause and are used for single stage, two-stage, DICS (not for U.S.), BRI, and PRI carrier access.
U	Use subaddress signaling method. The letter "U" may occur in the string only once and must not be in the final position. The "S", "P", "M", and "C" parameters cannot be used after "U".
N (n) (only for the U.S.!)	Network SFG (1 to 5) or Band Number (1).
L (for U.S. only!):	"L" must only occur at the end of a string of characters. "L" causes the call to be handled as an emergency call.
Network provider's method of access	Selection of the respective network provider
Unknown	No explicit specification about a network carrier.
Main network supplier	When seizing a trunk using the main network supplier, simplified dialing into the public network is performed by en-bloc dialing or by dialing individual digits.
MCL Single Stage	With MCL Single Stage, a prefix is used to dial the desired network carrier, and the station number is then dialed. Dialing occurs in the D channel for ISDN or as normal dialing for MSI.
MCL Two-Stage	With MCL Two Stage, a prefix is used to dial the desired network carrier. After a synchronization phase, a configurable authorization code is initially sent, followed by the destination call number as DTMF digits. With synchronization during timeout, you must program a pause of 2 to 12 seconds.
Corporate Network	A corporate network is directly connected to OpenScape Business. The LCR function determines the appropriate trunk group based on the station number dialed and then routes the call either via the trunk group in the public exchange or via the trunk group in the corporate network.
Dial-In Control Server	With this type of LCR, the desired network carrier is dialed with a prefix via a dial-in control server, and the call number and configurable authorization code are transmitted in the subaddress. Dialing occurs in the D channel.
Primary Rate Interface (PRI) (U.S. only)	In the case of the Primary Rate Interface, the selection of the network carrier or of a calling service is encoded in SETUP message using following information elements: Network Specific Facility, Operator System Access and Transit Network Selection.
Type	Type Of Number [TON];fFor each dial rule, the following types of number from "Called Party Number" can be selected from the drop-down list: PABX number, local area code, country code. "Unknown" is the default entry. The type of number is only set in E.164. In a network, parameters are set to "Unknown".

28.3.5.6 LCR > Multisite

Parameter Description of the Tab:

- **Change area**

Parameters	Description
Area Code	Enter the area code for a site (incl. a leading zero, e.g., `069` for Frankfurt and `030` for Berlin). Different area codes or even the same area code may be entered.
Area	Entry of the name for a site (e.g., the cities matching the area codes, i.e., `Frankfurt` and `Berlin`, for example, or department designations such as `Service` and `Sales` if the area code is the same).
Dedicated Route	Selection of the route or ITSP registration for this site.
Delete	Deletes the selected site entries.
Buttons	
Save	Saves the changes.

Parameter Description of the Tab:

- **Edit stations/groups**

Parameters	Description
Area	Selection of the site for the station or group.
Dedicated Route	Selection of the route or ITSP registration for the station or group.
Search	Search for stations and groups by entering the search term in the search fields **Call no**, **DID** or **Name** and then pressing the Return key. All stations and groups are listed if all search fields are left empty, and the Return key is pressed. The **Type** option can be used to display all station types (e.g., **SIP Clients** or **System Clients**).

28.3.6 Voice Gateway

The functions for IP telephony are grouped together under **Voice Gateway**.

28.3.6.1 Voice Gateway > SIP Parameters

Parameter Description of Tabs::

- **Edit SIP Parameters**

Parameters	Description
SIP Transport Protocol	

Parameters	Description
SIP via TCP	"Transmission Control Protocol". TCP is a mandatory transport protocol for SIP and cannot be deactivated here.
SIP via UDP	"User Datagram Protocol". UDP is the default transport protocol for SIP, but may be disabled if no endpoint/trunk/ITSP is using it. It is strongly recommended to keep UDP enabled.
SIP via TLS	"Transport Layer Security". TLS is the secure transport protocol for SIP and cannot be deactivated here.
SIP registrar	
Period of registration (sec)	Interval (in seconds) at which the registration of a SIP endpoint must be repeated. The value of the interval must not be set too high because registration is used to determine if an endpoint is out of service. (Registration period for ITSP trunks is configured in the ITSP profiles). Value range, default value: 10 - 86400, 120
RFC 3261 Timer Values	
Transaction Timeout (msec)	Specifies the wait time, in milliseconds, before a retransmission of the invite response for timer D for the RFC 3261 specification. This setting is relevant for the invite client transaction. Value range, default value: 2000 - 64000, 32000
SIP Session Timer	
RFC 4028 support	RFC 4028 defines an expansion of the Session Initiation Protocol (SIP). This expansion allows a periodic refresh of SIP sessions. The user agents and the proxies can use the refresh to determine, whether the SIP session is still active. The configuration option here is used to control the session refresh on the trunking interface (for ITSPs see the corresponding profile).
Session Expires (sec)	Defines the duration of a SIP session interval. The default value is "1800". The configured value is used for trunking and ITSP interfaces. Value range, default value: 90 - 65535, 1800
Minimal SE (sec)	Defines the shortest duration of a SIP session interval that is allowed. The configured value is used for trunking and ITSP interfaces. Value range, default value: 90 - 65535, 90
DNS Records	
Blocking time for unreachable destination (sec)	This timer is used to control the Blacklist of the SIP stack. If a SIP server resoved through DNS is unreachable it will be blocked for the time configured here. The default value is 60 sec. In cases where redundant servers are used (e.g. DNS results in multiple servers) a higher value is recommended (e.g. 900).
Provider Calls	
Maximum possible Provider Calls	The number of simultaneous calls via all activated providers is displayed here. This value is configured during setup depending on available bandwidth and ITSP configuration.

28.3.6.2 Voice Gateway > ITSP Loc-ID Settings

Parameter Description of Tabs:

- Add ITSP Location Info

  The ITSP location Info is used in the SIP protocol to inform the receiver of an emergency call about the geographical origin of the call. In the SIP protocol the format of location-ID info is defined RFC4119 & RFC5139 (XML coded Location object in the MIME body). The ITSP Loc-ID allows for defining all fields defined in the relevant RFCs whereas in your specific deployment only a subset of these data needs to be configured. (e.g. in Switzerland only the NAM field is used to define a location). The data required to define a location are provided by your ITSP.

Parameters	Description
Loc-ID Name	The name of the Location ID.
Country	The country is identified by the two-letter ISO 3166 code.
A1	National subdivisions (state, region, province, prefecture)
A2	County, parish, gun, district
A3	City, township, shi
A4	City division, borough, city district, ward, chou
A5	Neighborhood, block
A6	Street
PRD	Leading street direction
POD	Trailing street suffix
STS	Street suffix
HNO	House number, numeric part only
HNS	House number suffix
LMK	Landmark or vanity address
LOC	Additional location information
FLR	Floor
NAM	Name (residence, business or office occupant).
PC	Postal code
ROOM	Room
PLC	Place - type
PCN	Postal community name
POBOX	Post office box
ADDCODE	Additional Code
SEAT	Seat (desk, cubicle, workstation)
RD	Primary road or street

Parameters	Description
RDSEC	Road section
RDBR	Road branch
RDSUBBR	Road sub-branch
PRM	Road pre-modifier
POM	Road post-modifier
Activate Advanced Settings	When activated the advanced parameter fields can be configured.
BLD	Building (structure)
UNIT	Unit (apartment, suite)

28.3.6.3 Voice Gateway > Codec Parameters

Parameter Description of Tabs:

- **Edit Codec Parameters**

Parameters	Description
Codec	The parameters for the G.711 A-law, G.711 µ-law, G.729A and G.729AB codecs can be edited.
Codec: G.711 A-law	G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN). The A-law method is a digitization technique that is used primarily in Europe for analog audio signals in the telecommunications sector.
Codec: G.711 µ-law	G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN). In North America and Japan, the µ-law method, which is similar to the A-law, but not compatible, is used. In order to communicate, e.g., during a telephone conversation between Europe and the United States, the digital data must be translated through appropriate converters.
Codec: G.729A	Voice encoding at 8 Kbps.
Codec: G.729AB	Voice encoding at 8 Kbps. Speech pauses filled in with comfort noise.
Priority	The audio codecs can be assigned priorities between 1 (high) and 4 (low). The communication automatically tries to use the audio codec with the highest priority available for every connection. Using an audio codec with low voice compression (good voice quality) increases network load. In the case of intensive IP telephony, this can lead to diminished voice quality in a network already overloaded by data transfers.
Voice Activity Detection	Enable Voice Activity Detection (VAD). This can reduce network load during long voice pauses.

Parameters	Description
Frame Size	You can specify a frame size (IP packet size) of 10 to 90 msec for every codec. This specifies the sampling rate at which the audio codec splits the voice signal into IP packets. While a higher value (90 msec, for instance) results in a better relationship between payload and the IP packet overhead, it also increases the transfer delay. The adjustable values depend on the codecs. For networking of OpenScape Business with OpenScape Voice via SIP-Q V2: Cordless IP and OpenScape Mobile Connect only support a frame size of 20 ms for the G.711 codec. If one of these two products is present in the internetwork, the frame size must be to 20 ms here. Value range, default value: 10 - max. 90, 20
Enhanced DSP Channels	
Use G.711 only	Only the G.711 A-law and G.711 µ-law protocols are used. With G.711, fewer DSP resources are required, so more simultaneous calls are possible.
T.38 Fax	
T.38 Fax	Defines whether or not the T.38 Fax protocol is to be used. For system with Booster Card and/or Booster Server: When this flag is activated, error correction is performed in the T.38 protocol. A pop up window is displayed to notify the user that a manual System or OCAB / Booster Server restart is required.
Use FillBitRemoval	Defines whether or not fill bits should be deleted on sending and restored on receiving when using the T.38 Fax protocol. This makes it possible to save bandwidth.
Max. UDP Datagram Size for T.38 Fax (bytes)	Shows the maximum size of a T.38 UDP datagram in bytes. Value range, default value: 1 - 1472, 1472
Error Correction Used for T.38 Fax (UDP)	Defines which method is to be used for error correction. Values: t38UDPFEC, t38UDPRedundancy For system with Booster Card and/or Booster Server: When an option is selected, a pop up window is displayed to notify the user that a manual System or OCAB / Booster Server restart is required. Default value: t38UDPRedundancy
T.30 Fax	
Enable ECM	For system with Booster Card and/or Booster Server: When this flag is activated, error correction is performed in the T.30 protocol. A pop up window is displayed to notify the user that a manual System or OCAB / Booster Server restart is required. Default value: enabled
VoIP compatibility mode	For system with Booster Card and/or Booster Server: This flag should be activated if you encounter problems with fax transmission in VoIP networks. A pop up window is displayed to notify the user that a manual System or OCAB / Booster Server restart is required. Default value: disabled
Misc.	

Parameters	Description
ClearChannel	A ClearChannel is an open channel in which the endpoints are responsible for the protocol in the channel. The parameter defines whether or not the ClearChannel interface functionality is to be enabled.
Frame Size	You can set the sampling rate in this field. Possible settings are 10, 20, 30, 40, 50, and 60 milliseconds (msec). Value range, default value: 10 - 60, 20
RFC2833 RFC2833 defines how the tone signals are transmitted.	
Transmission of Fax/ Modem Tones according to RFC2833	Outband transmission (via SIP signaling); recommended operating mode to transmit tones securely
Transmission of DTMF Tones according to RFC2833	Outband transmission (via SIP signaling); recommended operating mode to transmit tones securely
Payload Type for RFC2833	Adaptation may be required, depending on the communication partner Value range, default value: 96 - 126, 98
Redundant Transmission of RFC2833 Tones according to RFC2198	Serves to increase the transmission reliability

28.3.6.4 Voice Gateway > Destination Codec Parameters

Priorities for the use of audio codecs can be defined for specific communication partners.

Parameter Description of Tabs::

- **Add Destination Codec Parameters**

Parameters	Description
Codec: G.711 A-law	G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN). The A-law method is a digitization technique that is used primarily in Europe for analog audio signals in the telecommunications sector.
Codec: G.711 µ-law	G.711 (A-law and µ-law): voice encoding at 56 or 64 Kbps - very high voice quality. G.711 is also used in fixed networks (ISDN). In North America and Japan, the µ-law method, which is similar to the A-law, but not compatible, is used. In order to communicate, e.g., during a telephone conversation between Europe and the United States, the digital data must be translated through appropriate converters.
Codec: G.729A	Voice encoding at 8 Kbps.
Codec: G.729AB	Voice encoding at 8 Kbps. Speech pauses filled in with comfort noise.

Parameters	Description
Priority	The audio codecs can be assigned priorities between 1 (high) and 4 (low). The communication automatically tries to use the audio codec with the highest priority available for every connection. Using an audio codec with low voice compression (good voice quality) increases network load. In the case of intensive IP telephony, this can lead to diminished voice quality in a network already overloaded by data transfers.
Destination	
Destination Address Type	Displays the type of destination to which the set priorities of the audio codecs are to be assigned.
IP address	IP address of the destination to which the set priorities of the audio codecs apply (e.g., networked node, SIP server)

28.3.6.5 Voice Gateway > Internet Telephony Service Provider

Parameter Description of Tabs:

- **Add Internet Telephony Service Provider**
- **Edit Internet Telephony Service Provider**
- **Delete Internet Telephony Service Provider**

Parameters	Description
Base Template	Selection of an empty template (default) or a predefined sample configuration for a particular service provider. This can be adapted to meet individual requirements and saved as a new ITSP.
Provider Name	Desired name of the ITSP. The configured ITSP will appear in the list of ITSPs under this name.
Enable Provider	The ITSP is activated.
Provider Identifier in System	Assignment of a unique designation in the system. A maximum of 8 ITSPs may be active simultaneously. Value range: Providers 1-8
Domain Name	Gateway Domain Name of the ITSP Often not identical with the web domain name.
Transport protocol	Desired transport protocol. UDP or TCP can be selected.
Transport security	The possible values are **traditional (upd or tcp)** for traditional call using udp/tcp or **secure (tls)** for secure call using TLS. Default value: **traditional (udp or tcp)**
Media security	The possible values are **RTP only** (only AVP profile is supported) or **SDES only** (only SAVP profile is supported). Default value: **RTP only**
Provider Registrar	
Use Registrar	Must be selected if the trunk works with registration (default = off).

Parameters	Description
IP Address / Host name	Host name or IP address of the external Registrar server.
Port	Port number of the external Registrar server, e.g., 5060. Enter port 00 if the ITSP uses DNSSRV.
Reregistration Interval at Provider (sec)	Interval (in seconds) at which ITSP registration is repeated. The value of the interval must not be 0 and must not be set too high because on repeating the registration at the ITSP, a dropped connection can also be detected, and an alternate route (via ISDN or an alternate Provider) may be selected if required. Default value: 120 seconds
Provider Proxy	
IP Address / Host name	Domain name or IP address of the proxy server (e.g., sip-voice.de). The entry is mandatory and is usually identical to the provider registrar entry.
Port	Port number of the proxy server (e.g., 5060). As a rule, this is identical with the Provider port number. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider Outbound Proxy	
Use Outbound Proxy	Only enable if the ITSP uses an outbound proxy that is different from the provider proxy. Disabled by default.
IP Address / Host name	Domain name or IP address of the outbound proxy.
Port	Port number of the outbound proxy. Enter port 0 if the ITSP uses multiple servers and DNSSRV.
Provider Inbound Proxy	
Use Inbound Proxy	Only set if the ITSP optionally sends requests from a second server. Disabled by default.
IP Address / Host name	Domain name or IP address of the second ITSP server
Port	Port number of the second ITSP server. Enter port 0 if the ITSP uses DNSSRV.
Provider STUN	
Use STUN	Only set if the ITSP uses a STUN server. The system-wide setting under the STUN configuration applies as the STUN mode for all ITSPs (default = off).
IP Address / Host name	Host name or IP address of the STUN server.
Port	STUN port number of the STUN server.
Extended SIP Provider Data	
Show Extended SIP Provider Data	By enabling this flag some additional configuration parameters are available to control the SIP stack and adapt the content of SIP header fields.

Parameters	Description
CLIP / CLIR	The system provides various parameters to control the format of SIP header fields according to the needs of the native trunk The contents of the following header fields which describe the source of a call can be controlled: • From: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>
CLIP outgoing in From header - display part	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in From header - user part:	Possible settings: • Call number • Account
Outgoing From Header - domain/ host part:	Change the domain / host part of the URI to be filled with the system's IP address. This parameter affects the host part of all three header fields From:, PAI and PPI Possible settings: • domain Name • local IP Address • public IP Address
Diversion: From contains original Calling Party Number:	If an outgoing call is established due to call forwarding, the system can provide information about the original calling party. If enabled the system sends the original calling party (A-Ext) in the From: header field, otherwise it sends the number of forwarding station.
Diversion: PAI contains original Calling Party Number	If an outgoing call is established due to call forwarding, the system can provide information about the original calling party. If enabled the system sends the original calling party (A-Ext) in the P-Asserted-Id header filed, otherwise it sends the number of forwarding station. Setting this flag the system sends the original calling party in the P-Asserted_ID: and P-Preferred-ID: header field.
CLIP outgoing in P-Asserted-Id header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name

Parameters	Description
CLIP outgoing in P-Asserted-Id header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in P-Preferred-Id header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in P-Preferred-Id header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in Diversion header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in Diversion header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in History-Info header - user part:	Possible settings: • omit • callnumber
CLIR outgoing in From header - display part:	Possible settings: • Omit • Call number • Account • Anonymous **From: Anonymous <sip: ...@...>**
CLIR outgoing in From header - user part:	Possible settings: • Call number • Account • Fully anonymous **From: ...<sip:anonymous@anonymous.invalid>** • User anonymous **From: ... <sip:anonymous@...>**
CLIR outgoing Privacy header	Possible settings: • Omit • Id **Privacy: id** • User **Privacy: user** • User, id **Privacy: user;id**

Parameters	Description
COLP / TIP supported for outgoing calls:	In ISDN the feature COLP (Connect Line Identification Presentation) was introduced. In SIP this feature is sometimes referred to as TIP (Termination Identification Presentation). RFD3324 (section 5.) defines a mechanism to transport the identity of the accepting party (C) in the P-Asserted-Identity header field of the 200 OK response: Possible settings: • COLP supported • COLP not supported
Call number formatting	
Incoming call - Called party number:	This flag refers to the destination address of a call. By default this is taken from the **user part** of the **TO: header** field. Possible settings: • Request line **INVITE sip: +498970070@...** • To header display part **To: +498970070 <sip:+** • To header user part **To: <sip: +498970070@...** • P-Called-Party-Id header display part **P-Called-Party-ID: +498970070 <sip:..** • P-Called-Party-Id header user part **P-Called-Party-ID: <sip: +498970070@..**
Incoming call - Calling party number:	This flag refers to the source address of a call. By default the system takes the calling party out of the From header user part. Possible settings: • automatic • From header display part **From: +498970070 <sip:+** • From header user part **From: <sip: +498970070@...** • P-Asserted-Id header display part **P-Asserted-ID: +498970070 <sip:..** • P-Asserted-Id header user part **P-Asserted-ID: <sip: +498970070@..** In automatic mode the system searches firstly in the user part of the P-Asserted-Identity, if present. If no P-Asserted-Identity is present, the user part of the From: header field is taken.

Parameters	Description
Incoming call - Type of number (calling):	Possible settings: • automatic • international
Incoming call - Type of number (called):	Possible settings: • automatic • international • national
Outgoing call - Type of number (calling):	Possible settings: • automatic • international • national
Outgoing call - Type of number (called):	Possible settings: • automatic • international • national
Mapping of provider number:	Possible settings: • in any case • Incoming called only (if configured) • off
CLIP no Screening support:	Possible settings: • not supported • CLIP in From / trusted number in PAI • Supported-No special treatment • CLIP in From / DID number in PAI
Call No. with international/national prefix:	Possible settings: • no • yes
Called number in E164 format:	Possible settings: • no • yes
Route optimization:	Possible settings: • not allowed • allowed • allowed (local IP in Contact)
MEX supported:	Possible settings: • no • yes

Parameters	Description
Contact URI contains:	This parameter is used to configure the user part content of the contact-URI **Contact: sip:UserPart@HostPart:port** Possible settings: • Call number: user part of the Contact URI contains the call number • Registration AOR: the Contact URI contains the account=user part of registration.
TCP port used in Contact URI:	This parameter is used to configure the tcp-port used in the host part of the contact-URI **Contact: sip:UserPart@HostPart:port** Possible settings: • ephem.src-port: Bydefault the ephemeral tcp src port is used • SIP server port: The SIP server port is used in the contact-URI
Registration	
Register Contact contains IP-Address:	Possible settings: • localIPAddr • domainName
ContactUriWithProtocol:	activate/deactivate
BNC Registration (SIPconnect):	Possible settings: • normal registration • BNC registration
ReRegistration interval after failure (sec):	
ReRegistration mode:	Possible settings: • continuous • SIPConnect
ReRegistration after call failure:	Possible settings: • CallFailureIsNoRegFailure • CallFailureIsRegFailure
Security	
UDP mode:	Possible settings: • symmetric UDP • asymmetric UDP
Approved Peer selection:	Possible settings: • trust configured Servers only • trust Servers received in SIP responses
Miscellaneous	

Parameters	Description
Direct Payload:	For a direct ITSP connection this parameter MUST be set to false. If an external SBC is used in front of the OpenScape Business this parameter is set to true.
Media Renegotiation Avoidance:	For a direct ITSP connection this parameter MUST be set to true. If the media handling parameter Direct Payload is set to true, this parameter has NO effect. (e.g., in cases where an external SBC is used in front of the OpenScape business system)
Change direction attribute:	Possible settings: • keep attribute • change to sendrecv
Silence Suppression attribute:	Possible settings: • supported • not supported
Mediasec extension:	Possible settings: • supported • not supported
SDP Filter:	Possible settings: • Default • Compatibility profile • Open
UseRouteURIAuthentication:	True sets the behavior for using the Route URI instead of the request URI in the (Proxy-) Authorization header for INVITE or INFO (not for REGISTER). The request URI will be used when no Route URI is present. For ITSPs this parameter MUST be set to true.
Ignore 100 Rel:	Ignore a 'Supported: 100rel' header field if received in INVITE. Because 100rel may interfere with interworking to non-SIP subscribers, this parameter SHOULD be set to true
Support 100rel	When setting this flag, the system will add a supported 100rel header in the outgoing invite. This will allow the ITSP to send reliable provisional responses followed by UPDATE messages. This parameter is useable for OpenScape Business V3 Mainboard family and Server without restriction.
UseViaRPort:	If set to true, the rport parameter is added to Via-Header. *Via: SIP/2.0/UDP 192.168.138.1:5060;rport;* If set to false, no rport parameter is added to Via-Header. *Via: SIP/2.0/UDP 192.168.138.1:5060;*

Parameters	Description
UPDATE Supported:	If set to true UPDATE is used depending on the contents of the Allow header field. If UPDATE is not set in the Allow header field received, the SIP stack never sends an UPDATE. If set to false, the UPDATE method will never be used (a re-INVITE is used instead of this) For ITSP this parameter SHALL be set to true (default)
P-Early-Media header support:	Possible settings: • not supported • supported
Session Timer support:	Possible settings: • not active • refresher Policy Remote
Send automatic 183 response timer (sec):	With this timer a provisional response (183) is triggered after timeout if no progress information is available from the system. This is necessary because some platforms do not stop supervision timers when receiving a 100 trying (e.g., Broadsoft) 0 no automatic response is sent; all responses are triggered by the system 1-10 timeout in sec, timer is started on receiving an INVITE request from the ITSP. On timer expiry a 183 is sent out by the SIP stack 0 (default)
UDP-Keep Alive:	Possible settings: • UdpKeepAliveON • UdpKeepAliveOFF • SendAliveOptions
Keep Alive interval for OPTIONS (sec):	With this parameter the interval for sending SIP OPTIONS is defined 60 (default)
Reregistration on OPTIONS Failure:	Possible settings: • NoRegisterOnFailure • RegisterOnFailure
Answer to OPTIONS:	Possible settings: • Full Answer • Without Body
Buttons	
Restart ITSP	Initiates a new registration with the ITSP (only possible with an activated ITSP).

Parameter Description of Tabs:

- **Edit STUN Configuration**

Parameters	Description
STUN Mode	This setting applies globally to all ITSPs, provided STUN is enabled for them. Whether STUN is needed or not depends on the ITSP infrastructure and the Internet router used. STUN is not required if the ITSP resolves NAT traversal on its own network. STUN ensures that the publicly accessible IP address is used in SIP messages instead of the internal IP address.
STUN Mode: Always	STUN is always active.
STUN Mode: Automatic	The NAT type of the router to the Internet is checked automatically. If STUN if required, it is enabled. If no STUN is required or possible, STUN is disabled. This is the recommended default setting.
STUN Mode: Use static IP	If the ITSP requires static IP authentication, a static IP address (public IP address) is required in the DSL modem or Internet router. The static IP address and port must be specified in addition.
STUN Mode: Use static IP, Public IP Address	Static IP address of the DSL modem or the Internet router.
STUN Mode: Use static IP, Public SIP Port	Port of the DSL modem or the Internet router.
STUN Mode: Port Preserving router	If none of the STUN modes mentioned above work, this mode should be tried. Some modems and Internet routers do not change the RTP port for NAT and need this mode for proper operation.
Detected Nat-Type	If an ITSP is active, the NAT type will be shown here.
Default STUN Server	
IP address / Host name	IP address or host name of the STUN server (e.g., `stun.serviceprovider.com`). This STUN server is used for SIP@Home when no ITSP is being used or if the used ITSP does not offer any STUN server.
Port	Port of the STUN server (e.g., `3478`)

Parameter Description of Tabs:

- **NAT Type Detection**

Parameters	Description
Automatic activation	Enables automatic detection of the NAT type.
Start NAT type detection	Starts the NAT type detection manually.

Parameter Description of Tabs:

- **Add Internet Telephony Station**
- **Edit Internet Telephony Station**
- **Delete Internet Telephony Station**

Parameters	Description
Internet Telephony Station	Access data of the account assigned by the ITSP. Depending on the ITSP, different designations are used for this, for example: SIP User, SIP ID, etc. You may also need to enter the ITSP customer number here. If static IP authentication is used, the PABX number must be entered here.
Authorization name	Authorization name assigned by the ITSP. This is often identical to the Internet telephony subscriber.
Password	Password assigned by the ITSP. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.
Confirm Password	Password assigned by the ITSP. Depending on the ITSP, different designations are used for this, for example: Password, SIP Password, etc.

Parameter Description of Tabs:

- **Add MSN Entry**
- **Edit MSN Entry**
- **Delete MSN Entry**
- **Delete All MSN Entries**

Parameters	Description
Internet Telephony Phone Number / **Internet Telephony Phone Number** / **Internet Telephony Phone Number**	(Single) Call number assigned by the ITSP.
DID / **Internal call number**	Assigned internal call number.
Default Entry	Activation as a default entry allows users who do not have their own Internet telephony phone number to make calls via this number. The option can be selected only for an MSN. (only for voice call support, not fax)
Internet Telephony Station / **Internet telephony station**	Displays the Internet telephony station

Parameter Description of Tabs:

- **Add DID Range**
- **Edit DID Range**
- **Delete DID Range**

Parameters	Description
PABX number	Head number assigned by the ITSP (without the DID number)
Direct inward dialing band from … to	Range of DID numbers assigned by the ITSP
Begin of internal Call Number range	First internal number as of which an automatic assignment of call numbers is desired.

Parameters	Description
Assign direct inward dialing band automatically to stations	If selected, the DID numbers are assigned automatically in ascending order to the internal call numbers, and the corresponding MSN entries are generated.

28.3.6.6 Voice Gateway > Networking > Nodes

Parameter Description of Tabs::

- **Add Networking Node**
- **Edit Networking Node**
- **Delete Networking Node**

Parameters	Description
Node ID	Only for manual configuration without a wizard, e.g., for open numbering: entry of a node number that is unique in the network.
IP address	Only for manual configuration without a wizard, e.g., for open numbering: IP address of the node
Node Monitoring	The selection of node monitoring causes a periodic review of the communication with the node. As a prerequisite, node monitoring must also be enabled in the other node.
Security Level of Node Encryption	Encryption for voice communication with the node is enabled by selecting "secure". To do this, "Signaling and Payload Encryption" must be additionally configured in the system. Value range: traditional, secure

28.3.6.7 Voice Gateway > Networking > Routing

Parameter Description of Tabs::

- **Add Call Number**
- **Delete all station numbers**

Parameters	Description
Node ID	Selects the node number
Phone number	Only for manual configuration without a wizard, e.g., for open numbering: entry of the code via which the node is reachable.

28.3.6.8 Voice Gateway > SIPQ-Interconnection

SIP-Q Interconnection is used to define the parameters for two possible external SIP-Q routes. Any external SIP server such as OpenScape 4000 or OpenScape Voice can be connected via these routes. Relevant examples are included in the existing templates.

Parameter Description of Tabs:

- **Add SIPQ-Interconnection**
- **Edit SIPQ-Interconnection**
- **Delete SIPQ-Interconnection**

Parameters	Description
Base Template	Template to be used as a base.
Name	Name of the external SIP server (template name).
Enable Trunk	The connection to the external SIP server is activated. Default value: disabled
Trunk Identifier in System	Selection between two external SIPQ-Interconnections. If present, one of the two SIPQ-Interconnections is always occupied by the UC Booster Card or UC Booster Server.
Remote Domain Name	Host name or IP address of the external SIP server. The value is typically identical to the value at **IP Address / Host name**.
SIP Server	
IP Address / Host name	Host name or IP address of the external SIP server.
Port	SIP port of the external SIP server. Value range: 0 or 1024 to 65535, default value: 5060
Secure Transport	When connected to OpenScape 4000 or OpenScape Voice, encrypted SIP signaling can be activated (Signaling and Payload Encryption feature). Default value: disabled
SIP Registrar	
Use Provider Registrar	The external SIP server requires registration. Default value: disabled
IP Address / Host name	Host name or IP address of the Registrar server.
Port	Port number of the Registrar server. Value range: 0 or 1024 to 65535, default value: 5060
Reregistration Interval (sec)	Interval (in seconds) at which the registration is repeated. Value range: 30 to 86400, default value: 300
Outbound Proxy/Inbound Proxy	
Use Provider Outbound/ Inbound Proxy	Activation of the outbound proxy: Some redundancy scenarios (e.g., with OpenScape Branch Proxy) require the handling of SIP signaling via an outbound proxy. Activation of the inbound proxy: In some redundancy scenarios (e.g., with OpenScape Voice), the incoming signaling occurs from a separate SIP server (inbound proxy). Default values: disabled in both cases

Parameters	Description
IP Address / Host name	Host name or IP address of the outbound or inbound proxy.
Port	Port number of the outbound or inbound proxy. Value ranges: 0 or 1024-65535

Parameter Description of Tabs:

- **Add SIPQ-Interconnection User**
- **Edit SIPQ-Interconnection User**
- **Delete SIPQ-Interconnection User**

Parameters	Description
UserId	Entry of the user ID for access to the SIP server.
Authorization name / **Realm**	Entry of the authorization name or realm for access to the SIP server.
Password	Entry of the password for access to the SIP server.
Confirm Password	Repetition of the password for access to the SIP server.

28.3.6.9 Voice Gateway > Native SIP Server Trunk

The parameters for the 10 possible external Native SIP routes are defined here. Any external SIP server can be connected via these routes.

Parameter Description of Tabs:

- **Add Native SIP Server Trunk**
- **Edit Native SIP Server Trunk**
- **Delete Native SIP Server Trunk**

Parameters	Description
Base Template	Template to be used as a base.
Trunk Name	Name of the external SIP server (template name).
Enable Trunk	The connection to the external SIP server is activated. Default value: disabled
Trunk Identifier in System	Choice of 10 external Native SIP connections. Grayed out items are occupied by already configured ITSPs (max 8 ITSPs possible - in this case, there are 2 Native SIP connections left).
Remote Domain Name	Host name or IP address of the external SIP server. The value is typically identical to the value at **IP Address / Host name**. Example: The configured **Remote Domain Name** is used in the Host part of From and PAI/PPI-header fields (see below): From: sip: +49...@DomainName P-Asserted-Identity: sip: +49...@DomainName

Parameters	Description
Transport protocol	Selection of the UDP or TCP protocol.
Transport security	Select between tranditional UDP or TCP and secure TLS.
Media security	Select between RTP only, SDES only and DTLS-SRTP. DTLS-SRTP is a protocol that combines Datagram Transport Layer Security (DTLS) with Secure Real-time Transport Protocol (SRTP) to provide encrypted and authenticated media streaming over the Internet. **NOTICE:** In new deployments (V3R4 onwards) DTLS-SRTP is default. Changing to DTLS-SRTP from either RT only or SDES only, requires a trunk restart for it to take effect. **NOTICE:** Restrictive firewall settings may cause sporadic or permanent voice payload issues. In that case, disable the DTLS-SRTP option.
SIP Server	
IP Address / Host name	Host name or IP address of the external SIP server.
Port	SIP port of the external SIP server. Default value: 5060, enter port 0 if the ITSP uses DNSSRV
SIP Registrar	
Use Registrar	Must be selected if the trunk works with registration (default = off)
IP Address / Host name	Host name or IP address of the external registrar server
Port	Port of the external registrar server default value: 5060, enter port 0 if DNSSRV is used
Reregistration Interval	The interval at which a registration is repeated (default = 600)
STUN Server	
Use STUN	Must be selected f the trunk works with STUN (default = off)
IP Address / Host name	Host name or IP address of the STUN server
Port	Port of the STUN server
Extended SIP Data	
Show extended SIP data	By enabling this flag some additional configuration parameters are available to control the SIP stack and to adapt the content of SIP header fields
CLIP / CLIR	The system provides various parameters to control the format of SIP header fields according to the needs of the native trunk The contents of the following header fields which describe the source of a call can be controlled: • From: DisplayPart <sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart <sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart <sip:UserPart@HostPart>

Parameters	Description
CLIP outgoing in From header - display part	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in From header - user part:	Possible settings: • Call number • Account
Outgoing From Header - domain/host part:	Change the domain / host part of the URI to be filled with the system's IP address. This parameter affects the host part of all three header fileds From:, PAI and PPI Possible settings: • domain Name • local IP Address • public IP Address
Diversion: From contains original Calling Party Number:	If an outgoing call is established due to call forwarding, the system can provide information about the original calling party. If set to true the system sends the original calling party (A-Ext) in the From: header field, otherwise it sends the number of forwarding station.
Diversion: PAI contains original Calling Party Number	If an outgoing call is established due to call forwarding, the system can provide information about the original calling party. If set to true the system sends the original calling party (A-Ext) in the P-Asserted-Id header filed, otherwise it sends the number of forwarding station. Setting this flag the system sends the original calling party in the P-Asserted_ID: and P-Preferred-ID: header field.
CLIP outgoing in P-Asserted-Id header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in P-Asserted-Id header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in P-Preferred-Id header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name

Parameters	Description
CLIP outgoing in P-Preferred-Id header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in Diversion header - display part:	Possible settings: • Omit - field is omitted • Call number - the number configured for a station. You can define which number is used in the "route parameters" • Account - the user name assigned to the native trunk • display name
CLIP outgoing in Diversion header - user part:	Possible settings: • Omit - field is omitted • Call number • Account
CLIP outgoing in History-Info header - user part:	Possible settings: • omit • callnumber
CLIR outgoing in From header - display part:	Possible settings: • Omit • Call number • Account • Anonymous **From: Anonymous <sip: ...@...>**
CLIR outgoing in From header - user part:	Possible settings: • Call number • Account • Fully anonymous **From: ...<sip:anonymous@anonymous.invalid>** • User anonymous **From: ... <sip:anonymous@...>**
CLIR outgoing Privacy header	Possible settings: • Omit • Id **Privacy: id** • User **Privacy: user** • User, id **Privacy: user;id**
COLP / TIP supported for outgoing calls:	In ISDN the feature COLP (Connect Line Identification Presentation) was introduced. In SIP this feature is sometimes referred to as TIP (Termination Identification Presentation). RFD3324 (section 5.) defines a mechanism to transport the identity of the accepting party (C) in the P-Asserted-Identity header field of the 200 OK response: Possible settings: • COLP supported • COLP not supported
Call number formating	

Parameters	Description
Incoming call - Called party number:	This flag refers to the destination address of a call. By default this is taken from the **user part** of the **TO: header** field. Possible settings: • Request line **INVITE sip: +498970070@...** • To header display part **To: +498970070 <sip:+** • To header user part **To: <sip: +498970070@...** • P-Called-Party-Id header display part **P-Called-Party-ID: +498970070 <sip:..** • P-Called-Party-Id header user part **P-Called-Party-ID: <sip: +498970070@..**
Incoming call - Calling party number:	This flag refers to the source address of a call. By default the system takes the calling party out of the From header user part. Possible settings: • automatic • From header display part **From: +498970070 <sip:+** • From header user part **From: <sip: +498970070@...** • P-Asserted-Id header display part **P-Asserted-ID: +498970070 <sip:..** • P-Asserted-Id header user part **P-Asserted-ID: <sip: +498970070@..** In automatic mode the system searches firstly in the user part of the P-Asserted-Identity, if present.If no P-Asserted-Identity is present, the user part of the From: header field is taken.
Contact URI contains:	This parameter is used to configure the user part content of the contact-URI **Contact: sip:UserPart@HostPart:port** Possible settings: • Call number: user part of the Contact URI contains the call number • Registration AOR: the Contact URI contains the account=user part of registration.
TCP port used in Contact URI:	This parameter is used to configure the tcp-port used in the host part of the contact-URI **Contact: sip:UserPart@HostPart:port** Possible settings: • ephem.src-port: Bydefault the ephemeral tcp src port is used • SIP server port: The SIP server port is used in the contact-URI

Parameter Description of Tabs:

- **Add Native SIP Server Trunk User**
- **Edit Native SIP Server Trunk User**
- **Delete Native SIP Server Trunk User**

Parameters	Description
UserId	Entry of the user ID for access to the SIP server.
Authorization name	Entry of the authorization name for access to the SIP server.
Password	Entry of the password for access to the SIP server.
Confirm Password	Repetition of the password for access to the SIP server.

28.3.7 Station

Functions for all stations are grouped together under **Station**. These include the name and phone number of the subscriber, for instance, as well as key programming information.

28.3.7.1 Station > Station > UP0 Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters
Name	Freely selectable name for the station. Value range: max. 16 characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits

Parameters	Description
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **UP0 Master/Slave**

  This tab appears only for OpenScape Business X8, since the slave ports are managed dynamically in this system. For OpenScape Business X1/X3/X5, the slave ports are assigned statically (i.e., are fixed)

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
Name	Freely selectable name for the station. Value range: max. 16 characters, no umlauts or special characters
Access	Displays the physical interface at which the device is connected.

Parameters	Description
Add Slave Zone	If this check box is selected, a slave port is preassigned to the selected master port. After saving the selection with **Apply** the call number, DID number and name of the slave system telephone can be configured in advance. When the slave system telephone is then connected to the slave adapter of the master system telephone, it is assigned the previously selected slave port. If the slave system telephone is connected without a predefined slave port, the next available port (as of port 384) is automatically used.
Delete Slave Zone	If this check box is selected, the preconfiguration of the slave system telephone is deleted. If a slave system telephone is already connected to the slave adapter of the master system telephone, the check box is grayed out, and the preconfiguration cannot be deleted.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Device Info**

Parameters	Description
Call no	Internal call number of the station.
Name	Station name.
Device type	Displays the device type associated with the station.
Current SW version	Software version of the associated device (if available).
HW version	Hardware version of the associated device (if available).
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.2 Station > Station > IP Clients

Parameter Description of Tabs:

- **Edit Subscriber**

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Type of the station.
Type: **No Port**	This call number is not yet assigned to any station.
Type: **System Client**	A system client is an IP station that can use all the features of the communication system via CorNet-IP (formerly called HFA system client)
Type: **RAS User**	A RAS user (Remote Access Service user) is granted Internet access to the IP network via the ISDN connection. This allows the communication system to be remotely serviced and licensed.
Type: **SIP Client**	A SIP client is an IP station that uses the SIP protocol. It can access only limited functionality of the communication system via SIP.
Type: **Deskshare User**	A Deskshare User is an IP user who can log in at another IP system telephone (mobile login) and then use this phone as his or her own phone (including the call number).
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Active	Indicates whether the station is operational.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
ITSP Loc-ID	The ITSP Location ID of a station.

Parameters	Description
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Enter key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Device Info**

Note that the sorting implementation is strictly alphabetic for all columns. There is no column-specific numerical sorting, for specific data types such as **IP Address** or **Current SW Version**.

Parameters	Description
Call no	Internal call number of the station.
Display	Station name.
Device type	Displays the device type associated with the station.
IP Address	IP address of the associated device; direct link to the WBM of the IP telephone
MAC Address	MAC address of the associated telephone
Current SW version	Software version of the associated device (if available).
HW version	Hardware version of the associated device (if available).
PC Port	If this flag is enabled, the PC Ethernet port is switched on at all active system telephones. Default: disabled

Parameters	Description
Codec Setting	If this flag is enabled, the following codec prioritization applies to all system telephones: G.729 - G.711 - G.722 If this flag is disabled, the following codec prioritization applies: G.722 - G.711 - G.729 **NOTICE:** CP100 does not support G.722 Default: disabled
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Secondary Gateway**

Parameters	Description
Call number	Internal call number of the station.
Name	Station name.
NodeId	Each node in a networked system must be assigned a unique node ID. This enables the individual nodes in a networked system to be uniquely identified.
Fallback telephony	Indicates if the feature is activated.
Fallback Call No	The call number of the station that will be used in case of a failure event.
Fallback Call No DID	The internal call number of the station that will be used in case of a failure event.

Parameter Description of Tabs:

- **Fallback Hosting**

Parameters	Description
Call number	Internal call number of the station.
Name	Station name.
Primary NodeId	The unique node ID to which the staation is originally configured.
Fallback Call No	The call number of the station that will be used in case of a failure event.
Fallback Call No DID	The internal call number of the station that will be used in case of a failure event

28.3.7.3 Station > Station > Analog Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station. **NOTICE:** Call numbers starting with a star (*) cannot be used as fax destinations.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.

Parameters	Description
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.4 Station > Station > ISDN Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.

Parameters	Description
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.5 Station > Station > DECT Stations > SLC Call number

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.
Device type	Displays the device associated with the subscriber. Base stations are shown as S0 stations.

Parameters	Description
Access	Displays the physical interface at which the device is connected.
ITSP Loc-ID	The ITSP Location ID of a station.
Parameters	Default view for all stations; do not change the settings
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.6 Station > Station > DECT Stations > DECT Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Active	Indicates whether the station is operational.

Parameters	Description
Device type	Displays the device associated with the subscriber.. DECT stations are shown as Comfort-PP.
Fax Call no.	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Fax DID	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Access	Displays the physical interface at which the device is connected.
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.7 Station > Station > IVM/EVM Ports > EVM

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the voicemail port.
DID	DID number of the voicemail port, if present.
First Name	Freely selectable first name for the voicemail port. Value range: max. 32 characters.
Last Name	Freely selectable last name for the voicemail port. Value range: max. 32 characters.

Parameters	Description
Display	Freely selectable name for the voicemail port. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA).
Active	Indicates whether the voicemail port is operational.
Device type	For EVM, S0 stations are displayed.
Access	Displays the internal port for the voicemail.
ITSP Loc-ID	The ITSP Location ID of a station.
Station type	"PhoneMail" must be selected for EVM; "Standard" should be set for the Company AutoAttendant.
Parameters	Default view for all voicemail ports; do not change the settings (e.g., the "language" is not the language of voicemail announcements).
Search	You can also have selected voicemail ports displayed by entering a search term in the **Search** fields and pressing the Return key. The voicemail ports that match the search term are displayed. If you leave all the **Search** fields empty and press the Return key, all voicemail ports will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.8 Station > Station > Virtual Stations

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the virtual station.
DID	DID number of the virtual station.

Parameters	Description
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Empty or virtual station (fixed display for Mobility Entry)
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA)
Active	Indicates whether the virtual station is operational.
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.9 Station > Station > Station Parameters

Parameter Description of Tabs:

- **Edit station parameters**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.

Parameters	Description
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Direct inward dialing	DID number of the station.
Device type	Displays the device associated with the subscriber.
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Access	Displays the physical interface at which the device is connected.
Device Provisioning	This menu is only visible to SIP stations and the following values are available: • **Standard** (default value) • **Mitel SIP DECT Device** (The specific SIP device is used for the Mitel SIP DECT). **NOTICE: Mitel SIP DECT Device** option is only supported on V3 hardware and OSBiz S systems.
Mitel SIP DECT Configuration: This menu becomes visible only when **Mitel SIP DECT Device** is selected under **Device Provisioning**.	
PIN	The PIN code of the device.
Key Lock Enabled	Enable (Yes) or disable (No) the device key lock.
Key Lock PIN	The PIN for the key lock.
Key Lock Time	The time for the key lock to take effect.
Show Personal Directory	Choose whether the personal directory is visible (Yes) or not (No).
Fax	
Call number	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from internal locations can be received by the subscriber should be entered here.
Direct inward dialing	If a fax box has been set up (e.g., with the UC clients myPortal for Desktop or myPortal for Outlook), the fax number at which fax messages from external locations can be received by the subscriber should be entered here.
Mobility	

Parameters	Description
Type	Type of the station: • Mobility station • Virtual station • SFB station • Trusted external station: virtual station type to be used in order to create a Trusted external user
Mobile/Sfb/Trusted external station call number	Only for SIP clients and mobile users: For the One Number Service, this number is used for the authentication of DISA access via the mobile service. Enter the mobile phone number associated with the subscriber together with the dialout prefix (i.e., the CO code), e.g., 0017312345678). **NOTICE:** The **Trusted external station call number** field is mandatory. If you proceed to apply the configuration with the **Trusted external station call number** field empty then an alert will pop up, informing you that "*Trusted external station call number must not be empty!*". Additionally, after you click **OK** on the first alert, a second one will pop up, informing you that "*The input could not be handled, please check*".
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry only) and "automatic" (internal call number of the subscriber) or selection of the station number of the client or phone from the drop-down list.
Parameters	
Station type	Type of the connected device (drop-down list)
Station type: **Standard**	System telephones or analog telephones
Station type: **Fax**	Fax machine, e.g., no override possible
Station type: **Loudspeaker**	For paging via the a/b port
Station type: **Answering Machine**	Only for analog: if an answering machine is connected to this interface, this setting enables a call to be taken over from the answering machine from any device even though the answering machine has already accepted the call. To do this, the terminal must be programmed with the internal call number of the analog station. Besides being selected for answering machines, this entry should also be selected for virtual ports where no physical equipment has been set up. This prevents the communication system from checking the operating status of the port. Only for virtual ports: If a station without access was configured as a type of answering machine in Manager E, the port must be additionally configured as a virtual port. Otherwise, it will not be visible as a station in the WBM.
Station type: **P.O.T. MW LED**	For standard analog telephones (P.O.T = Plain Old Telephone) with a message-waiting LED Not for U.S.

Parameters	Description
Station type: **Door station with pulsed loop**	When using a pulsed loop device with the door opener function
Station type: **Modem**	Call override is not possible with this setting. It is intended for modems.
	When a fax or modem station is deleted (i.e., the call number and DID are deleted), the extension type must also be reset to the default (standard).
Language	Language for the menu control of the device (system telephone).
Call signaling internal	Every station can be assigned one of a total of eight possible internal ringing tones here. This means that in addition to the external ringing tone, an internal ringing tone is assigned here and subsequently transmitted for internal calls. Default value: Ring type 1
Call signaling external	Three different ring types for signaling external calls can be selected here: – System Phones: Ring type 1 = External call (e.g., double ring), Ring type 2 = External call CO 2 (e.g., triple ring), Ring type 3 = External call CO 3 (e.g., short/long/short) – Analog telephones for Germany: Ring type 1 = External call, Ring type 2 = Automatic recall, Ring type 3 = Door bell ring – Analog telephones for other countries: Ring type 1 = External call, Ring type 2 = External call, Ring type 3 = External call Default value: Ring type 1
Class of Service (LCR)	A subscriber can only seize a route if his or her COS is greater than or equal to the LCR COS in the route table, i.e., a subscriber with a COS 7 cannot seize a route with COS 8. By default, all subscribers are entered with the maximum LCR Class of Service (15). Default value: 15
Hotline Mode	Selection of the hotline options
Hotline Mode: **off**	Disables the hotline feature.
Hotline Mode: **Off-hook alarm after timeout**	The call to the hotline takes place after a predefined delay (off-hook alarm time), see Telephony/Basic Settings/System/Intercept-Attendant-Hotline
Hotline, Mode: **Hotline**	Enables the hotline feature. On lifting the handset, the connection to the hotline destination is established immediately, see Telephony/Basic Settings/ System/Intercept-Attendant-Hotline
Hotline	For details on selecting hotline destinations, see Telephony/ Basic Settings/ System/Intercept-Attendant-Hotline
Hotline: **none**	No destination defined
Hotline: **Digits 1 to 6**	For details on hotline destinations, see Telephony/ Basic Settings/System/ Intercept-Attendant-Hotline
Payload Security (for IP system clients)	Enable or disable the encryption of phone conversations (SPE). To do this, all stations involved must have SPE enabled. Default value: on

Parameters	Description
Payload Security (for TDM/ Analog telephones)	Indicates if the specific endpoint is secured or not from infrastructure perspective as payload security works only for IP telephones. If this parameter is set to on and SPE Support system flag is activated, it is displayed whether or not the connection path between this station and an IP station is encrypted. If the parameter is set to off the no information is displayed. Default value: off
MWI protocol	Selection of MWI protocol for analog stations. Available only for SLMAVx (OpenScape Business X8), 4SLAV onboard and SLAVx OpenScape Business X3,X5.
MWI protocol: Comtel3	Comtel 3 protocol selected. Default value.
MWI protocol: High Voltage	High Voltage protocol selected. Available only for SLMAVx (OpenScape Business X8).
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit station flags**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Station flags	
Override class of service on	When this flag is activated, the subscriber can intrude into (i.e., override) an internal subscriber's ongoing connection. The subscribers involved are notified of the busy override by a warning tone and a display message. Default value: Disabled
Override Do Not Disturb	When this flag is activated, the following applies: when the subscriber calls a station for which Do Not Disturb has been activated, he or she can override Do Not Disturb. After five seconds, the call is signaled at the called station. If the flag is disabled, the Do Not Disturb function cannot be overridden. Subscribers who call a station for which Do Not Disturb has been activated receive the busy tone. Default value: Disabled

Parameters	Description
FWD external permitted	When this flag is activated, the subscriber can activate call forwarding to an external destination. Charges incurred for the execution of an external call forwarding are allocated to the subscriber who activated the call forwarding. Default value: Enabled
Prevention of voice calling off	When this flag is activated, the station can be called directly. This enables an internal call to be set up without lifting the handset. The loudspeaker on the called station is activated automatically in the process. Default value: Enabled
DISA class of service	When this flag is activated, external subscribers can activate or deactivate functions of the communication system via DISA (Direct Inward System Access) and set up outbound external connections just like any other internal subscribers. This also includes activating and deactivating call forwarding, the Do Not Disturb feature and the lock code, for example. Default value: Disabled
Transit allowed via Hook-on	When this flag is activated, the subscriber can transfer an external call to another external subscriber by hanging up. Example: The subscriber is the conference controller and hangs up: if there are other internal subscribers still in the conference, the longest participating internal subscriber automatically becomes the conference controller. If there are only external participants remaining in the conference, the conference is terminated, and all connections are cleared. Default value: Disabled
System telephone lock reset	When this flag is activated, the subscriber can reset the individual lock code of other internal subscribers to the default code. Default value: Disabled
CLIP analog (only for analog devices)	When this flag is activated, the caller's phone number is shown on the phone display of the analog station. As a prerequisite, the analog phone of the subscriber must support CLIP (Calling Line Identification Presentation). Default value: Enabled
MCID access	When this flag is activated, the subscriber can have malicious external callers identified via the ISDN Central Office. As a prerequisite, the "Trace call" (Malicious Call Identification, MCID) feature must have been applied for and activated by the network provider. After the "Trace call" feature has been activated by the network provider, the following must be noted: for each incoming call from the ISDN CO, the release of the connection to the called station is delayed for a specific timeout period after the caller hangs up. This timeout enables the called station to activate the "Trace call" feature. The ISDN trunk availability is somewhat reduced as a result. Default value: Disabled
Entry in telephone directory	When this flag is activated, the name and number of the subscriber will be displayed in the system directory (including ODS). Default value: Enabled

Parameters	Description
Editing the Telephone Number	When this flag is activated, the subscriber can edit the digits of the call number entered via the keypad before the digit transmission. This requires a system phone with a display. Default value: Disabled
No group ringing on busy	When this flag is enabled, the following applies: The status of the station with group ringing programmed (i.e., the primary station) determines whether or not group ringing occurs. If the primary station is free, all stations included in the group are called immediately. If call waiting is enabled at the primary station: all stations included in the group are called after a delay of 5 seconds. If the primary station cannot receive a call or if call waiting is inactive: group ringing does not take place. Default value: Disabled
Associated dialing/services	Associated dialing: when this flag is activated, the subscriber can dial a number on behalf of another internal subscriber as if that station itself were dialing. Associated services: When this flag is activated, the subscriber can control features on behalf of another internal subscriber as if that station itself were controlling these features. This includes activating and deactivating call forwarding, group ringing and the lock code, for example. Default value: Disabled
Call waiting rejection on	When this flag is activated, subscribers who are conducting a call are not informed about other incoming calls via a call waiting tone or a display message. Default value: Enabled
Discreet call	When this flag is activated, the subscriber can discreetly join an existing voice call of another internal subscriber. He or she can silently monitor the call and speak with the internal subscriber without the other party hearing this conversation. This is only possible in the case of a two-party call. Discreet calling is not possible with consultation calls or conferences. Default value: Disabled
Discreet Call Lock	When this flag is activated, the station cannot be called discreetly. Default value: Disabled
DTMF-based feature activation	Only relevant for Mobility Entry stations: This flag must be set in order to be able to activate features during a call (i.e., in the talk state). The code receiver remains active. (Attention: limited resources) Default value: Disabled
Headset	When this flag is activated, the station can be equipped with a headset that plugs into the handset connection. Setting the flag enables the user to accept a call by pressing a headset button on the system telephone without lifting the handset. When a headset is connected to the system telephone connection, it is recognized automatically by the communication system; an authorization enable is not necessary in this case. When this flag is set, calls cannot be released by pressing the speaker key; a disconnect key must be programmed so that calls can be released. Default value: Disabled

Parameters	Description
Last destination mailbox active	If this flag is activated and the called party is not available, the call is forwarded to the substitute mailbox, and the caller's number is displayed on the substitute telephone. Default value: Disabled
Call prio./immed. tone call wait.	When this flag is activated (Call priority/immediate tone call waiting), calls through this station are signaled with a higher priority to partners. The priority is set to be the same as the priority of external calls. In other words, the prioritized calls are thus queued before existing internal calls, but after existing external calls. Note that existing first calls (not waiting calls) are usually never displaced, regardless of their ring type. If the same priority is also to be set for an internal call in another node, then the station flag "Call prio./immed. tone call wait." (Area: Circuit flags, Call prio./immed. tone call wait.) must be likewise set for the corresponding trunk. If this flag is set, the caller receives a ring tone immediately instead of a busy tone. This has no impact on the acoustic signaling. The prioritized calls are still signaled like an internal call. This feature is important for phonemail connections. Default value: Disabled
Voice recording	If the flag is activated, the subscriber can activate voice recording during a call. In addition, the **Warning tone during voice recording** switch under Flags can be used to specify whether or not a warning tone should be output on starting the voice recording. Furthermore, a suitable Live Recording device must be configured under PhoneMail. Default value: Disabled
Compress display data	When this flag is enabled, the display outputs are compressed for improved performance. If the display on a UP0/E terminal changes, the communication system only updates the data that differs from the previous display. If an application (e.g., Smartset/TAPI) is connected via an RS 232 adapter (data or control adapter), this feature must be deactivated. The flag must be deactivated for applications that obtain the call number information from the telephone's display, (i.e., uncompressed output with call number instead of compressed output with name). Names are generally displayed only when the flag "Calling ID only" under "Display name/call number" is deactivated. Default value: Enabled
Door release DTMF	If this flag is enabled, the station can open a door with the DTMF/MFV code signaling when a door relay is connected to the relevant port. Default value: Disabled
Autom. connection, CSTA (only for OpenStage SIP telephones)	When the flag is enabled, the following applies: speakerphone mode is activated on the associated SIP telephone when dialing or answering calls via myPortal or myAttendant. The information contained in the documentation of the SIP telephone must be observed, since additional settings on the SIP phone may be required for the proper use of the feature. When the flag disabled, the call setup occurs only after lifting the handset. Default value: Enabled

Parameters	Description
Disable handsfree microphone	If this flag is activated, the handsfree microphone cannot be used. This flag is only supported by OpenStage phones. Default value: Disabled
Forced Number Presentation	If this flag is activated, the caller's phone number appears on the display of the called party instead of his or her name. Default value: Disabled
Usage (for specific countries only)	This drop-down list can be used to configure the output current of the interfaces of an analog board (in mA, e.g., 27 mA for China).
Operating Mode	In this drop-down list, an operating mode can be selected for the subscriber line.
Missed Calls List	When this flag is activated, the missed calls list is activated for the subscriber at his or her telephone (only for phones with a display). Calls that were not answered by the subscriber are provided with a time stamp (time and date) and added to a chronologically sorted list. Only the calls which also contain a phone number or name are recorded. If a subscriber calls more than once, only the time stamp for the entry is updated, and a call counter for that caller is incremented.
Central busy signaling	This flag must be set (see also QSIG features) for subscribers who have busy signaling on a centralized communication system. Does not apply to the USA. The implementation of central busy signaling is contingent on a maximum number of 100 stations per node.
Display of Emergency text	If this flag is activated, a configurable Emergency text is shown on the phone's display in emergency mode.
Call Supervision	When this flag is activated, the subscriber can silently monitor (i.e., listen in on) the conversation of any internal subscriber. The microphone of the party listening in is automatically muted. The monitored subscriber is not notified via a signal tone or display message. When you start and end call supervision, you may encounter a lapse of up to two seconds of the conversation. Default value: Disabled
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit workpoint client data**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.

Parameters	Description
Name	Station name.
Parameters	
Status message	For system clients only: this flag activates the "keep-alive" mechanism for system telephones. If a system phone fails, for example, it is flagged as inactive after four minutes. The flag must not be enabled when setting up a system telephone as a home client or when using the "Short-Hold" feature. Disabling this flag reduces the message traffic between the communication system and the system telephones.
Authentication active	If you want the IP client to be able to identify itself at the communication system with a password, authentication must be activated and a password set. This is an advantage especially for clients that are not connected to the internal LAN, but that dial in from outside. For SIP clients only: You have to enter a password. The same password must be used in device.
New password	Password for authentication. For SIP clients only: If device password has been already set, same password must be used upon Apply to keep device registration on.
Confirm password	Password to repeat the authentication.
SIP User ID / Username	Only for SIP clients: freely selectable user name for authentication of the SIP subscriber, e.g., "SIP-120". The value defined here must also be entered at the SIP telephone.
Realm	Only for SIP clients: freely selectable names for the associated zone, e.g., "OSBIZ-SIP". This value must be the same for all SIP clients. The value defined here must also be entered at the SIP telephone.
Fixed IP address	For SIP clients only: entering a fixed IP address ensures that only one SIP client can log on to the system with this IP address. If this flag is activated, the IP address and the call number are verified. If this flag is not activated, only the call number is verified.
IP Address	Only for SIP clients: IP address of the SIP client (e.g., the IP address of the SIP telephone)
Type	Only for system clients: A mobile IP client (Mobile option) is not permanently assigned to any IP phone. The call no. of a mobile IP client can be used by a subscriber to log on to any IP terminal (that permits this) via the logon procedure (*9419) (provided the option Mobile blocked is not activated).
Type: **Mobile**	Only for system clients: No IP device is permanently assigned to the subscriber. The feature is only supported from the third station port onwards.
Type: **Non-mobile**	Only for system clients: The call number is permanently assigned to the IP device of the subscriber. When using a WLx phone, the option Non mobile must be set before registering the WLx phone with the communication system.
Type: **Non-mobile and blocked**	Only for system clients: A subscriber cannot log into this IP device with a mobile system client.

Parameters	Description
Blocked for Deskshare User	Only for system clients: This system phone can be shared by multiple subscribers (Desksharing).
Secondary system ID	This parameter has two different functions: 1. For all stations: defines the multi-location gateway assigned to the station. 2. Only for system clients: If the "Emergency" flag has been set (under the "Stations/ IP Clients/Secondary Gateway") for networked systems, the node ID of the failover system for system clients can be entered here.
Internet registration with internal SBC	Enables the SIP@Home feature. This makes it possible for an external STUN-enabled SIP phone to register at OpenScape Business over the Internet and thus be used as an internal telephone.
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

Parameter Description of Tabs:

- **Edit Group/CFW**

Parameters	Description
Stations - ...	
Type	Type of the station.
Call number	Internal call number of the station.
Name	Station name.
Call forwarding	
Day destination	Displays the call forwarding destinations for incoming external calls during the day (see the wizard User Telephony/Call Forwarding)
Night destination	Displays the call forwarding destinations for incoming external calls during the night (see the wizard User Telephony/Call Forwarding).
Internal destination	Displays the call forwarding destinations for incoming internal calls (see the wizard User Telephony/Call Forwarding).
Class of Service	
Day	Every subscriber can be assigned a class of service for day. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Night	Every subscriber can be assigned one class of service for night. There are 15 classes of service to choose from (see Telephony/Classes of Service).
Call Pickup	
Group	Every station can be assigned to a call pickup group. You can choose between 32 call pickup groups (120 with OpenScape Business S; see also Incoming Calls / Call Pickup).

Parameters	Description
Buttons	
>	Moves to the next station. If the stations matching the search term entered in the **Search** fields were previously filtered, it is possible to move between only those specific stations.
<	Skips back one station.

28.3.7.10 Station > Station > UC Applications

The functions of the UC solutions UC Smart and UC Suite are shown here. It is recommended that the basic settings be configured under "Setup > Basic Installation> Basic Installation> Change preconfigured call and functional numbers".

Depending on the UC solution being used, different functions are displayed.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Call number of the service
DID	DID number of the service
First Name	Freely selectable first name for the service. Value range: max. 32 characters.
Last Name	Freely selectable last name for the service. Value range: max. 32 characters.
Display	Freely selectable name for the service. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Depending on the UC solution: UC Smart: MeetMe / Conference UC Suite: Auto-Attendant / Fax / Contact Center Fax / Park / MeetMe / Conference / Fax Group
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) **NOTICE:** CLIP is not supported for UC fax. It is only supported for analog fax.
Active	Indicates whether the service is operational.

Parameters	Description
ITSP Loc-ID	The ITSP Location ID of a station.
Search	You can also have selected services displayed by entering a search term in the **Search** fields and pressing the Return key. The services that match the search term are displayed. If you leave all the **Search** fields empty and press the Return key, all services will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.11 Station > Station > Profiles/Templates

User profiles (with user parameters, station flags, Groups/RNA, etc.) can be set up here as an way to create default settings for multiple users simultaneously.

Parameter Description of Tabs:

- **Edit All Profiles**

Parameters	Description
Profiles	Displays the profile number.
Name	Input of any profile name.

Parameter Description of Tabs:

- **Display All Profile Users**

Parameters	Description
Profiles	Displays the profile number.
Name	Displays the profile name.
Member Call no	Displays the internal call number of the profile member.
Member Name	Displays the name of the profile member.

Parameter Description of Tabs:

- **Add/Delete Profile member**

Parameters	Description
Profiles - ...	Displays the profile number.

Parameters	Description
Name	Displays the assigned profile name.
Profile Members	
Selection	List of subscribers available in the system.
Members	List of subscribers assigned to the profile.
Buttons	
Add	Add selected subscribers from the selection list to the list of profile members.
Delete	Delete selected member from the list of profile members.

Parameter Description of Tabs:

- **Import/Export Profile**

Parameters	Description
Load Profile via HTTP	
Remote File Name (PC File System)	Load an existing profile file in XML format
Export Profile via HTTP	
File name	Display the file name under which the profile is output (XML format)
Action	Download the profile
Buttons	
Reset Default Values	The profile values for all subscribers assigned to this profile are reset to the default values.

Parameter Description of Tabs:

- **Import/Export All Profiles**

Parameters	Description
Load All Profiles via HTTP	
Remote File Name (PC File System)	Load an existing profile file. Multiple profiles may be stored in this file.
Export All Profiles via HTTP	
File name	Display the file name under which the profiles are stored.
Action	Download the profile in a profile file.
Buttons	
Reset Default Values	The profile values for all profiles and assigned subscribers are reset to the default values.

Parameter Description of Tabs:

- **Edit station parameters: see > Station > Stations > Station Parameters**

- **Edit station flags: see > Station > Stations > Station Parameters**
- **Edit Group/CFW: see > Station > Stations > Station Parameters**

28.3.7.12 Station > Station > DID Extensions

Displays an overview of the configured DID numbers with the associated subscribers.

Parameter Description of Tabs:

- **Display DDI Extensions**

Parameters	Description
Call no	Displays the call number of the station.
Name	Displays the name of the station.
DID	Displays the DID number of the station.
(additional fields can be displayed)	

28.3.7.13 Station > Station > Mobility Entry

It is recommended to set up mobile users via the "User Telephony > Mobile Phone Integration" wizard.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Input of the internal extension number of the Mobility user (e.g., 777). This internal call number must not have already been assigned.
DID	Input of the internal DID number of the Mobility user. This internal DID number must not have already been assigned.
First Name	Freely selectable first name for the Mobility user. Value range: max. 32 characters.
Last Name	Freely selectable last name for the Mobility user. Value range: max. 32 characters.
Display	Freely selectable name for the Mobility user. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Type	Displays the type of Mobility user.
Device Type	Displays the system telephone type associated with the image file.

Parameters	Description
Clip/Lin	Sequence of digits to be displayed at the called party instead of the actual number for outgoing external calls (e.g., for E911 emergency services in the USA) Value range: max. 16 digits
Access	Displays the physical interface at which the device is connected.
Mobile CallNo	Input of the mobile phone number. The entry must include the leading dialout prefix (i.e., the CO code), e.g., 0016012345678.
Web Feature ID	The Web Feature ID defines how the subscriber should log in at the mobile web client (user name). Choice between "no" (Mobility Entry user without myPortal to go) and "automatic" (internal call number of the subscriber or Mulap) or selection of the station number of the client or phone from the drop-down list.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

Parameter Description of Tabs:

- **Secondary Gateway**

  Only for networked systems (multi-location)

Parameters	Description
Call number	Internal call number of the Mobility User.
Name	Name of the Mobility User.
Node ID	Input of the node ID via which the mobile subscriber is externally accessible.

28.3.7.14 Station > Station > SfB User

Parameter Description of Tabs:

- **Edit Subscriber**

Parameters	Description
CallNo	Input of the internal extension number of the Skype for Business Client Mobility User (e.g., 777). This internal call number must not have already been assigned.
DID	Direct inward dialing number of the Skype for Business Client.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters.
Type	Displays the type of Mobility User, which in this case is always SfB Station.
SfB Call Number	The Skype for Business Client call number.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **CallNo** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.15 Station > Station > Overview of Stations

Lists all stations of the communication system sorted by call number (default). Clicking on a different column heading sorts the list by the selected column in ascending order; a second click sorts it in descending order.

Parameter Description of Tabs:

- **Change Station**

Parameters	Description
Call no	Internal call number of the station.

Parameters	Description
DID	DID number of the station.
First Name	Freely selectable first name for the station. Value range: max. 32 characters.
Last Name	Freely selectable last name for the station. Value range: max. 32 characters.
Display	Freely selectable name for the station. By default, it is created using the First Name and Last Name parameters depending on display name algorithm. Value range: max. 16 characters, no umlauts or special characters
Device type	Displays the type of station.
Active	Indicates whether the station is operational.
Access	Displays the physical interface at which the device is connected.
Search	You can also have selected subscribers displayed by entering a search term in the **Search** fields and pressing the Return key. The subscribers who match the search term are displayed. If you leave all the **Search** fields empty and press the Enter key, all subscribers will be listed again.
Items per page	Selection to determine whether 10, 25, 50 or 100 items are to be displayed per page.
Buttons	
Blue arrow in the **Call no** column	Brings up the page with the **Edit station parameters**, **Edit station flags**, **Edit workpoint client data** and **Edit Group/CFW** tabs.
>	Moves one page forward.
<	Moves one page back.
>|	Moves to the end of the list.
|<	Moves to the beginning of the list.

28.3.7.16 Station > Key Programming

Parameter Description of Tabs:

- **Program Keys**

  Key programming is supported only for UP0 phones and HFA clients. Search function (by Callno, DID, First Name, Last Name, Display and Device Type filelds) is available.

Parameters	Description
Selection list	Selection of subscriber's telephone.
Shift Layer	If a key has been set up with the "Shift Layer" function, the second level can be programmed here

Parameters	Description
telephone	Clicking on the key area of the phone opens the current key assignment.
Keypad	Displays the key function (function key label)
Key button	Selection of the desired function

Parameter Description of Tabs::

- **Copy keypad for other stations**

Parameters	Description
Copies the key layout from the station	Selection of the station whose key layout is to be copied for the selected stations
All stations	Copy the key layout to all stations.
Selection field	Copy the key layout to the selected stations
Station	Displays the internal call number and the name of the station.
Device Type	Displays the phone type of the subscriber. Device type cannot be changed for already Active stations.
Copy the device type from station	Selection of the station whose device type is to be copied for the selected stations
to the following station(s)	Selection of the station(s) in which the device type will be copied. Filtering by the device type of the stations is available.

28.3.8 Cordless

Functions for the integrated cordless solution for the operation of cordless telephones (DECT phones) via the communication system are grouped together under **Cordless**. The base stations and DECT phones (internal stations with HFA features) are configured here.

28.3.8.1 Cordless > System-wide

Parameter Description of Tabs:

- **Edit system-wide data**

Parameters	Description
CMI data	

Parameters	Description
System ID	Entry of the 8-digit, hexadecimal DECT system ID. This is supplied on purchasing the DECT system. It is composed as follows: 1st. digit: E/ARC (Access Right Class) 2nd.-5th. digit: EIC (Equipment Installer's Code) 6th.-7th. digit: (FPN Fixed Part Number) 8th digit (Fixed Part Subscriber, FPS)
Freq. band	Selection of country-specific frequency band. By default, the frequency band assigned to the entered country code is displayed.
Speech coding	Displays the system-wide voice codec (a-law, µ-law).
Encryption	Encryption is the encoding of the data at the air interface and can be activated or deactivated. Default: active
Login window	Opening time of the login window for the registration of DECT phones. The login window is opened by entering the code *94 2 19970707 and the password at a system telephone. The call numbers of the DECT phones to be registered are then entered in the Login window. Default: 10 minutes
Echo Handling These parameters can be used to disable the echo handling set under **Trunks** > **Parameters/General Flags** for mobile stations on a node-wide basis. The settings are made in accordance with the line settings of the calls. Potential improvements by general deactivation or line-specific activation must be tested in individual cases.	
Echo Suppressor	The Echo Suppressor (ES) inserts an attenuator in the receive direction of the DECT phone, depending on its transmit level. If the echo suppressor is turned on in cases where there is loud extraneous noise, it is conceivable that the receive signal may be further dampened. This could adversely affect the clarity of the call. In the **"not active"** mode, the receive direction of the DECT phone is not attenuated when the DECT phone has a high transmit level. In the case of analog trunk switching and loud environments, this setting can offer improved clarity of the trunk station at the DECT phone. Default: Automatic
Echo Canceller	The Echo Canceller (EC) eliminates unwanted signal echoes caused by a 4/2-wire conversion (fork) on the land line. If the Echo Canceller is activated without an echo, errors may occur, since the Echo Canceller attempts to adapt to a non-existent echo. In the "**not active**" mode, the activation of this parameter is prevented, and the Echo Canceller is always off. Default: Automatic

Parameters	Description
Artificial Echo	The Artificial Echo Path (AE) echoes back an attenuated voice signal (24dB) from the land line to the remote subscriber. This may be needed in the case of an international connection, for example, to provide an inserted echo canceller with a certain preload. In the "**not active**" mode, the activation of this parameter is prevented, and the Artificial Echo is always off. Default: Automatic
PP Deviation Control	Echoes often occur when VoIP calls are made using DECT phones.The "PP Deviation Control" function can be activated to suppress/minimize these echoes. This function affects all DECT handsets connected to the communication system. The activation or deactivation only takes affect for a handset when it is turned off and turned back on. In the **"not active"** mode, echo suppression does not work, and echoes can occur when VoIP connections are made using DECT handsets. Default: not active
Economic Mode	
Economic Mode	The ECO mode can be enabled system-wide for all DECT phones. In ECO mode, the transmit power of DECT phones is either reduced by a fixed value (static) or every DECT phone adjusts its transmit power independently to the received signal strength (adaptive). Default: not active
Economic Mode: **Off**	The ECO Mode is disabled system-wide.
Economic Mode: **On**	The ECO mode (static) is enabled system-wide. The transmit power of the DECT phones is reduced by a fixed value.
Economic Mode: **Adaptive**	The ECO mode (adaptive) is enabled system-wide. Every individual DECT phone adjusts its transmit power independently to the received signal strength. During a handover, the system first switches to the high transmit power and then reduces the transmit power, depending on the reception.

28.3.8.2 Cordless > SLC

Parameter Description of Tabs:

- **Change DECT Station**

Parameters	Description
Call no	Call number of the DECT phone.
DID	Direct inward dialing number of the DECT phone.
Name	Name of the DECT phone.

Parameters	Description
Active	Logon status of the DECT phone: Green: The DECT phone is active. Red: The board lockout switch was set for a logged-on DECT phone. Yellow: The DECT phone was automatically logged off on changing the PIN. Gray: No DECT phone has ever been logged on at this port.
Mobile code	PIN code to log on the DECT phone. The mobile code must be unique throughout the system.
Access	Name, number and slot of the S_0 extension cable.
Slot	Displays the slot of the plugged in SLC board.
Buttons	
Delete	The DECT phone is removed from the system. In other words, the call number, DID number and name are deleted, and the associated TDM user license is released.

Parameter Description of Tabs:

- **Add DECT Station**

Parameters	Description
System ID	If the communication system is not part of an internetwork (node ID = 0), the system identifier is preset to 1. If the communication system belongs to an internetwork (node ID > 0), the system ID must match the node ID (**Cordless** > **Multi SLC** > **System ID**).
Slot	Slot of the plugged SLC board.
SLC No.	Unique system-wide ID number of the SLC board. Range of values: 1-15,17-31,33-47,...,127. Multiples of 16 are not allowed.
Number of DECT phones	Number of already configured DECT phones of this SLC board.
SLC Call number	Unique system-wide call number of the S_0 extension line.
Access	Name, number and slot of the S_0 extension cable.
Add DECT Station	
Number of DECT phones	If the number of DECT phones is less than the size allowed in the system (which depends on the version), an additional number of DECT phones can be added for this SLC board here. The newly added DECT phones are displayed under the **Edit DECT Stations** .

28.3.8.3 Cordless > Multi-SLC

Parameter Description of Tabs:

- **Edit Multi-SLC**

Parameters	Description
SLC No.	Unique system-wide ID number of the SLC board. Range of values: 1-15,17-31,33-47,...,127. Multiples of 16 are not allowed.
Node ID	Displays the node ID (if configured). If the communication system is part of an internetwork, all configured SLC boards of the internetwork are displayed here.
SLC Call number	Unique system-wide call number of the S_0 extension line of the SLC board. Value length: maximum 5 digits

28.3.8.4 Cordless > Base Stations

Parameter Description of Tabs:

- **Edit base station**

Parameters	Description
Slot	Displays the slot in which the SLC board of base station is inserted. Slot 2 is displayed for the mainboard (SLUC).
Type	Type of base station. In the case of an SLC board, the type is only displayed; for SLUC, the type can be selected. If the type is changed from **No Port** to **Base station**, 16 DECT phones are automatically preconfigured, and an SLC networking line is set up.
Type: **Base station**	Base station connected.
Type: **No Port**	No base station connected.
Name	Name of the base station.
Level	Level of the base station. Range of values: 50% and 100%; default value: 100%
Status	Status of the base station.
Master port	For an SLC board, the ports to which the base station is connected are displayed. For an SLUC board, all ports with the connected terminal devices are displayed.

28.3.9 Incoming calls

Call Management (CM) functions are grouped together under **Incoming calls**. These include settings for groups, for instance, and call forwarding-no answer.

28.3.9.1 Incoming Calls > Groups/Hunt groups

For the initial configuration of group calls and hunt groups, it is recommended that the **Group Call / Hunt Group** wizard be used.

Parameter Description of Tabs:

- **Edit Group Call Numbers**
- **Display Used Groups**
- **Display all group members**
- **Add group**
- **Delete group**
- **Edit group parameters**
- **Display members**
- **Add member**
- **Edit member order**
- **Check Basic MULAPs**
- **Check MULAP Preference**

Parameters	Description
Index	Consecutive number that is assigned by the communication system.
Call no.	Phone number of the group call, hunt group, basic MULAP, executive MULAP or voicemail group
DID	DID number of the group call, hunt group, basic MULAP, executive MULAP or voicemail group
First Name	Freely selectable first name for the group call, hunt group, basic MULAP, executive MULAP or voicemail group. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the group call, hunt group, basic MULAP, executive MULAP or voicemail group. Value range: max. 16 characters, no umlauts or special characters
Display	Name of the group call, hunt group, basic MULAP, executive MULAP or voicemail group By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
Type	Definition of the group type Default value: Group For more information see: Table: Type options
Ring type	Defines the acoustic signaling of incoming external calls to the group Default value: 1 Only the default setting is possible for analog phones. Changes have no effect.
Ring type: 1	Two rings
Ring type: 2	Three rings
Ring type 3	short-long-short ring
Tel. directory	When this flag is activated (Display Yes), the call number of the group appears in the internal directory. Default value: Enabled

Parameters	Description
Mulap as group member	When this flag is activated, the MULAP group can be added as a member in Groups.
Group member	
Group	Number (index) of the group
Member	Number (index) of the member within the group
Call number	Call number of the group member
Name	Name of the group member
Parameters	Enabled parameters of the group member
Parameter: M	Master (M): Basic MULAP: The member is master of the basic MULAP. Executive MULAP: The member has Executive functions.
Parameter: R	Acoustic call (R): Basic MULAP and Executive MULAP: Incoming calls are signaled acoustically.
Parameter: A	Automatic seizure outgoing (A): Basic MULAP: The Basic MULAP trunk is automatically selected for a call when you lift the handset. Executive MULAP: The Executive MULAP trunk is automatically selected for a call when you lift the handset.
Parameter: K	No automatic incoming call acceptance (K): Basic MULAP and Executive MULAP: An incoming call must be accepted by pressing the MULAP key.
Parameter: P	Automatic privacy release (P): Basic MULAP and Executive MULAP: You can release the seized MULAP line for a conference by pressing the MULAP key.
MULAP key set up	Indicates whether or not a MULAP key has been configured the group member.
Route	For an external member of the group, the route is displayed.
Group	
Consistency Check	Possible collisions due to the overlapping of masters of basic MULAPs or in the automatic outgoing seizure of basic MULAPs are displayed.

Table 63: Type options

Parameters	Description
All group type conversions are allowed without deleting group members, excluding MULAP group types. **NOTICE:** If a group of type *Group*, *Linear hunt group*, *Cyclical hunt group* or *Voicemail* has a MULAP group as member, then conversion to type *RNA Group* or *Call Waiting Group* is not allowed. **NOTICE:** If a group member sets call forward (*1) to another *Hunt Group*, *Call Waiting Group* and *RNA Group*, the call is not routed. This is disallowed to avoid call loops. For direct calls to the station the forwarding is valid. For *Cyclic* and *Linear Group (Hunt Group)* members this is allowed, *1 to any destination works - except for voicemail.	
Type: Linear hunt group	An inbound call is always signaled first at the first member of a hunt group. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.
Type: Cyclical hunt group	An inbound call is always signaled first at the member that follows the subscriber who answered the last call. Further signaling is performed on the basis of the sequence in which the members are entered in the group table.
Type: Group	Group call of type Group: Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. If all group members are busy, a call is signaled by a camp-on tone. Call signaling continues at all group members (camp-on tone at busy group members) even if the subscriber hangs up.
Type: RNA	Group call of type RNA: Incoming calls are simultaneously signaled at all group members. If a group member is busy, the entire group call is marked as busy (only the busy members are signaled for the incoming call). Callers of the group receive the busy signal.
Type: Basic MULAP	Incoming calls are indicated visually at all phones associated with the basic MULAP (Multiple Line Appearance). The subscriber can also set whether or not incoming calls should also be acoustically signaled for each individual member. The status of the Basic MULAP changes to busy and other callers hear the busy signal when a call is answered. The Basic MULAP phone number is shown on the called party's display for outgoing calls via the Basic MULAP trunk.
Type: Executive MULAP	You can configure Executive MULAPs if you want to use restricted executive and secretary functions. If a caller rings the Executive MULAP phone number, the call is visually signaled at all phones belonging to the Executive MULAP. Incoming calls are also signaled acoustically for members with secretary functions.
Type: Call waiting	Group call of type Call Waiting: Incoming calls are simultaneously signaled at all available group members. Available group members are subscribers who are not busy. A call is signaled by a camp-on tone for busy group members.

Parameters	Description
Type: Voicemail	Voicemail group: A voicemail group enables a specific group of subscribers to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail box (i.e., the voicemail) of the group and not to the group members. After a voicemail is left in the voicemail box of the group, it is forwarded to the voicemail boxes of all members. All members receive the voicemail simultaneously. Whenever a member deletes a voicemail, this voicemail is also deleted from the voicemail boxes of all members and the voicemail box of the group. The personal voicemails of all members are not affected by this.

28.3.9.2 Incoming Calls > Group Members

Parameter Description of Tabs::

- **Edit member**
- **Delete member**

Parameters	Description
Group	Number (index) of the group
Group member	Number (index) of the group member
Phone number	Call number of the group member
First Name	Freely selectable first name for the group member. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the group member. Value range: max. 16 characters, no umlauts or special characters
Name	Name of the group member By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
MULAP name	MULAP (Multiple Line Appearance) group name. This is the MULAP name that is displayed on the phone display when this Team group is called. The MULAP name is the same for all Team group members that have the same type.
MULAP call no.	MULAP group number
Master (M)	Basic MULAP: Activating this flag changes a member into a master of the Basic MULAP. If a master activates call forwarding, this feature applies to all members (phones) in the Basic MULAP. Executive MULAP: Activating this flag assigns executive functions to a member. The Executive MULAP trunk is automatically selected for a call when you lift the handset. Incoming calls via the Executive MULAP phone number are only signaled visually.

Parameters	Description
Acoustic call (R)	Basic MULAP and Executive MULAP: When this flag is activated, incoming calls are signaled acoustically. Default value: Enabled for all masters of a Basic MULAP. Activated for all members with the Secretary function of an Executive MULAP.
Automatic seizure outgoing (A)	Basic MULAP: When this flag is activated, the Basic MULAP trunk is automatically called when the subscriber lifts the handset. Executive MULAP: When this flag is activated, the Executive MULAP trunk is automatically called when you lift the handset. Default value: Enabled for all masters of a Basic MULAP. Activated for all members with the Secretary function of an Executive MULAP.
No automatic incoming call acceptance (K)	Basic MULAP and Executive MULAP: When this flag is activated, you cannot answer an incoming call by lifting the handset. Answering an incoming call is possible only by pressing the MULAP key. Default value: Disabled
Automatic privacy release (P)	Basic MULAP and Executive MULAP: When this flag is activated, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key. Default value: Disabled
MULAP key set up	Basic MULAP: When this flag is activated, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Basic MULAP trunk. The Basic MULAP number appears on the called party's display. Executive MULAP: When this flag is activated, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display. Default value: Enabled
Route	For an external member of the group, the route is displayed.
Type	Definition of the group type

28.3.9.3 Incoming Calls > Team/top

For the initial configuration of Team and Top groups, it is recommended that the **Team Configuration** and **Executive / Secretary** wizards be used.

Parameter Description of Tabs::

- **Display All Team/top**
- **Display Used Team/top**
- **Add Team/top Group**
- **Edit Team/top Group**
- **Delete Team/top Group**
- **Edit Team/top Group**

- **Display Team/top Members**
- **Add Team/top Member**
- **Edit Team/top Member**
- **Delete Team/top Member**
- **Display Fax Boxes**
- **Add Fax Box**

Parameters	Description
Index	Consecutive number that is assigned by the communication system.
First Name	Freely selectable first name for the Team/Top group. Value range: max. 16 characters, no umlauts or special characters
Last Name	Freely selectable last name for the Team/Top group. Value range: max. 16 characters, no umlauts or special characters
Name	Name of th Team/Top group By default, it is created using the First Name and Last Name parameters depending on display name algorithm.
Type	Definition of the group type
Type: Team	A Team Group offers several convenient team functions. The station numbers of all team members are programmed on MULAP keys (trunk keys). Every team member can thus access all trunks (for instance, for call pickup) and can also conduct calls simultaneously via multiple trunks.
Type: Top	A Top Group offers convenient Executive and Secretary functions (Top function) for up to three executives and up to three secretaries.
Team as group member	This flag is configurable only when the Team Group has members with the same station type, which results in a single MULAP group below this Team Group. When this flag is activated, the MULAP group can be added as a member in Groups.
Key assignment to team	Definition for the setup of MULAP keys of Team Group members
Key assignment to team: to first/second console	When this flag is activated, an automatic setup of MULAP keys occurs on the first or second add-on device (key module or BLF) of the Team telephone.
Key assignment to team: to first free key	When this flag is activated, an automatic setup of MULAP keys occurs on the first free key of the Team telephone.
Key assignment to top	Definition for the setup of MULAP keys of Top Group members
Key assignment to top: to first/second console	When this flag is activated, an automatic setup of MULAP keys occurs on the first or second add-on device (key module or BLF) of the Top telephone.
Key assignment to top: to first free key	When this flag is activated, an automatic setup of MULAP keys occurs on the first free key of the Top telephone.
Group member	
Group	Number (index) of the group
Members	Number (index) of the member within the group

Parameters	Description
Type	Definition of the member type
Call no.	Call number of the group member (changes in a MULAP group to ** Call no and is internally accessible under this ** Call no.)
Name	Name of the group member
MULAP call no.	MULAP group number
MULAP DID	DID number of the MULAP group
MULAP name	MULAP group name. This is the MULAP name that is displayed on the phone display when this Team group is called. The MULAP name is the same for all Team group members that have the same type.
Ring type	Defines the acoustic signaling of incoming external calls to the group Default value: 1 Only the default setting is possible for analog phones. Changes have no effect.
Ring type: 1	Two rings
Ring type: 2	Three rings
Ring type 3	short-long-short ring
Tel. directory	When this flag is activated (Display Yes), the call number of the group appears in the internal directory. Default value: Enabled
Master (M)	Team group: Activating this parameter turns a member of the Team group into a master of the group. If a master activates call forwarding, this feature applies to all members (phones) in the Team group. Top group: Enabling this flag assigns Executive functions to a member. The Executive MULAP trunk is automatically selected for a call on lifting the handset. Incoming calls via the associated Executive MULAP phone number are only signaled visually by default.
Acoustic call (R)	Team group and Top group: When this flag is activated, incoming calls are signaled acoustically. Default value: Enabled for all members of a Team group. Activated for all members with the Secretary function of a Top group.
Automatic seizure outgoing (A)	Team group and Top group: When this flag is activated, a call is automatically made via the MULAP trunk of this member on lifting the handset. Default value: Enabled
No automatic incoming call acceptance (K)	Team group and Top group: When this flag is activated, you cannot answer an incoming call by lifting the handset. Answering an incoming call is possible only by pressing the MULAP key. Default value: Disabled

Parameters	Description
Automatic privacy release (P)	Team group and Top group: When this flag is activated, you can release the seized MULAP line for a conference by pressing the MULAP key. The release of this line is signaled to all other members by the flashing MULAP key. They can join the conference by pressing the MULAP key. Default value: Disabled
MULAP key set up	Team group: When this flag is activated, a MULAP key is programmed on the associated phone. Pressing the key sets up an outgoing call via the MULAP trunk of the master. The MULAP station number of the master appears on the called party's display. Top group: When this flag is activated, a MULAP key is programmed on the associated phone. You can press the key to set up an outgoing call via the Executive MULAP trunk. The Executive MULAP phone number appears on the called party's display. Default value: Disabled for all members of a Team group. Enabled for all members of a Top group.
MULAP type	Definition of the MULAP type
MULAP Type: Basic MULAP	Incoming calls are indicated visually at all phones associated with the basic MULAP. The subscriber can also set whether or not incoming calls should also be acoustically signaled for each individual member. The status of the Basic MULAP changes to busy and other callers hear the busy signal when a call is answered. The Basic MULAP phone number is shown on the called party's display for outgoing calls via the Basic MULAP trunk.
MULAP type: Executive MULAP	All members of an Executive MULAP can be reached at the Executive MULAP phone number as well as at their personal station numbers.
Fax Call no.	Call number of the group member's fax box
Fax DID	Direct inward dialing number of the group member's fax box

28.3.9.4 Incoming Calls > Call Pickup

Parameter Description of Tabs::

- **Edit names of call pickup groups**
- **Display Selected Group**
- **Edit Selected Group**

Parameters	Description
Group	
Group	Number (index) of the call pickup group Value range: 1 to 32 (120 for OpenScape Business S)
Name	Name of the call pickup group
Station	

Parameters	Description
Call no.	Call number of the internal station
Name	Name of the internal station
Allocation Group X	If the flag is activated, the station is assigned to the call pickup group X.
Group	Call pickup group to which this station is assigned.

28.3.9.5 Incoming Calls > UCD

Parameter Description of the Tab:

- **Edit UCD Parameters**

Parameters	Description
UCD flags	
Allow UCD applications	When this flag is activated, the Uniform Call Distribution (UCD) feature is released throughout the system Default value: Enabled
Agents permanently available	When this flag is activated, all UCD agents are permanently available agents. A permanently available agent will then remain available for calls, faxes and e-mails even when he or she does not accept a call, fax or e-mail. Default value: Disabled
Automatic wrap-up time	
Wrap-up time (cycles)	The automatic wrap-up time for all UCD agents is defined on a system-wide basis in ring cycles, that is, in increments of five seconds. During the wrap-up time, an agent is temporarily removed from the call distribution in order to allow the agent some time to wrap up the call just completed. Default value: 0
Priorities for internal calls	
Priorities, internal	System-wide definition of priority for internal calls based on 10 priority levels (1 = high, 10 = low). Default value: 10
Priorities for external calls	
Slot / line	Displays the board, the slot and the number of the line (B channel). Priorities are assigned on the basis of trunks for external calls (per B channel), regardless of whether IP or TDM lines are involved.
Priority	Defines the priority for external calls received on the relevant line (B channel). The definition is based on 10 priority levels (1 = high, 10 = low). Default value: 1

Parameter Description of Tabs:

- **Display UCD Groups**
- **Edit UCD Group**

Parameters	Description
Call number	Call number of the UCD group
MSN	DID number of the UCD group
Name	Name of the UCD group
Prim. ring cycles	Definition of the primary ring cycle: This is defined in ring cycles, that is, in increments of five seconds. This setting specifies how long a call remains in the queue if not accepted by the agent longest in "available" state. The call is then forwarded to the next available agent. Default value: 3 Cycles
sec. ring cycles	Definition of the secondary ring cycle: This is defined in ring cycles, that is, in increments of five seconds. This setting specifies how long a call remains in the queue if not accepted by the next available agent. Default value: 3 Cycles
Queued Calls	Definition of the maximum number of queued calls: When the maximum number of queued calls is reached, further calls can be forwarded to an overflow destination (which may be an external destination, another UCD group, an internal station or a group). Default value: 10 (Default value of the last UCD group: 72)
AICC	Definition of the Automatic Incoming Call Connection (AICC). This setting applies to all agents in a UCD group, irrespective of whether or not the agent's phone features a headset. Default value: No
AICC: yes	The agents in this UCD group can accept calls without any additional operating steps. An audible tone notifies the agent via the headset about an incoming call that is then automatically put through.
AICC: no	The agents in this UCD group can accept incoming calls only when using conventional operations (for example, by lifting the handset).
Ann. change	Definition of possible announcement changes Default value: once
Ann. change : single	The queued caller will receive a one-time announcement.
Ann. change : cyclical	The last announcement and the second to last announcement in the configuration are repeated cyclically.
Overflow time	Definition of the overflow time in seconds: If a queued call is not accepted by the UCD application within the overflow time, the call is processed further by the communication system in accordance with the Call Management specifications. This setting is relevant only when an external UCD application is connected. Default value: 600

Parameters	Description
Announcement Delay Time	Definition of the announcement delay in seconds: after this time has elapsed, a queued caller receives an announcement. Default value: 0

Parameter Description of the Tab:

- **Edit UCD Group Parameters**

Parameters	Description
Dest. index	For each UCD group, up to seven destinations (index 1 to 7) for announcements can be defined. The announcements of the destinations are played to the queued caller sequentially.
Announcement equipment	Announcement for the relevant destination index.
Wait time	The announcement can be played either cyclically (max 9 cycles with 5 sec each = 45 sec) or in an continuous loop. After this time, the announcement of the next index is played to the caller in the queue (not in the case of a **continuous** loop). Default value: endless

Parameter Description of the Tab:

- **Add-Delete UCD Group Members**

Parameters	Description
Selection	List of all UCD agent IDs. The UCD agent IDs do not correspond to the call numbers in the communication system.
Members	List of UCD agent IDs of the selected UCD group
Buttons	
Add	Adds the selected UCD agent IDs of the UCD group.
Delete	Deletes the selected UCD agent IDs from the UCD group.

Parameter Description of the Tab:

- **Assign Stations**

Parameters	Description
Agent ID	List of UCD agent IDs of the selected UCD group.
Stations	List of stations that can be assigned to the UCD agent IDs of the UCD group.

28.3.9.6 Incoming Calls > Call Forwarding

Parameter Description of Tabs::

- **Call dest. list - Definition**

Parameters	Description
Call dest. list	Selection of the call destination list to be processed. Value range: 1 to 740
Edit Call Forwarding To find a call destination faster, you can also enter one or more digits in the **Target 1 - Target 4** fields. This takes you directly to the list item that starts with the specified string of digits. It is also possible to enter a character string.	
Target 1 - 4: **No entry**	The call destination is skipped.
Target 1 - 4: **External destination**	Route and external phone number with CO access code.
Target 1 - 4: *** Dialed station**	Called subscriber.
Target 1 - 4: **** User-defined**	Destination of call forwarding after timeout (if configured).
Target 1 - 4: **#9 System search**	Next available station (except for Executive extensions).
Target 1 - 4: **#201 - #260**	Call Distribution (UCD Group).
Target 1 - 4: **#801 - #817**	Ann. device.
Target 1 - 4: 100, 101, ...	Call number of a subscriber or a group (e.g., voicemail box)
Call forwarding starts after	Time after which a call is forwarded to the next call destination. For UCD groups, call forwarding is based on the mechanisms of the primary and secondary call cycles (see UCD groups). Range of values: 5/10/15/...75 s; default value: 15 s
Call Forwarding	The call is immediately forwarded to the next call destination "on busy". Default value: enabled
Second ringer	
Second ringer destination	Additional internal station at which the call is also signaled or an actuator (relay) of an actuator/sensor assembly for a common ringer (night bell).
Second ringer type	The call can be signaled at the station immediately or after the entire call forwarding time has expired. Default value: Immediately

Parameter Description of Tabs::

- **Call dest. list - Assignment**

Parameters	Description
Call no	Call number of the subscriber or group.
Name	Name of the subscriber or group.
Type	Subscriber Type, e.g., U_{P0}, system client, AB, ISDN, SIP.

Parameters	Description
Day	Call destination list number to be used for incoming external calls during business hours (day service) Default value: 14
Night	Call destination list number to be used for incoming external calls during night service Default value: 15
Internal	Number of the call destination list for incoming internal calls Default value: 16
Search	Entering a search term in the **Call no** or **Name** search fields and then pressing the return key causes all hits containing the specified search term to be displayed. For example, entering the call number `521` would display the matches `+495213535` and `+498967521`, and entering the term `co` as the name would display `Collins`, `Mcoin` and `Branco`. Pressing the return key with nothing entered in any of the search fields causes all entries to be displayed.

Parameter Description of Tabs:

- **Members of dest. list**

Parameters	Description
Show all members with call destination list	Displays all subscribers or groups that are using the selected call destination list.

Parameter Description of Tabs:

- **Copy call dest. lists**

Parameters	Description
Call dest. list	Selects the call destination list to which subscribers are to be assigned. Value range: 1 to 740
Day	Call destination list to be used for incoming external calls during business hours (day service)
Night	Call destination list to be used for incoming external calls during night service
Internal	Call destination list for incoming internal calls
Call dest. lists	
Selection	List of all subscribers.
Members	List of subscribers to whom the call destination list is assigned.
Buttons	
Add	Transfers the selected subscribers from the Selection window to the Members window.
Delete	Deletes the selected subscribers from the Members window.

28.3.10 Trunks/Routing

The functions for trunks and routes are grouped together under **Trunks/ Routing**.

28.3.10.1 Trunks/Routing > Trunks

Parameter Description of Tabs:

- **Display all lines**
- **Change Route**

Parameters	Description
Trunk	Display of the physical CO trunk connected to the communication system.
Box-SI-Pt-Li or Box/Slot/ Port/Line	Displays the card type and the slot and port number (physical port) where a specific trunk is connected to the communication system.
Code	Display or setup of the seizure code On entering this number, the communication system seizes the trunk assigned to it. It is used to test the trunk or to program a line key. If CSTA applications are used, the value for this parameter should be set.
Route	Display or selection of the route that is assigned to the trunk (none or Trk. Grp 1 to Trk. Grp 12). If "none" is set in this column for an active trunk, system behavior will not be stable. Also, the system can receive a call on this trunk but the call cannot be forwarded.
Status	Displays the line status. Inactive lines are flagged with an asterisk.
Type	Displays the line type. Inactive lines are designated as "No Port".

Parameter Description of Tabs:

- **display ringing assignment all lines**

Parameters	Description
Trunk	Display of the physical CO trunk connected to the communication system.
Box-SI-Pt-Li or Box/Slot/ Port/Line	Displays the card type and the slot and port number (physical port) where a specific trunk is connected to the communication system.
Day call no.	Displays the call number assigned for day service
Day name	Displays the name of the assigned call number for day service
Night call no.	Displays the call number assigned for night service
Night name	Displays the name of the assigned call number for night service

Parameter Description of Tabs:

- **Add line**

Parameters	Description
Number	Number of trunks to be added.

Parameter Description of Tabs:

- **Change direction**

Parameters	Description
Line	Displays the number of the line.
outgoing	Outgoing calls may be made on the line. **NOTICE:** Emergency calls can be made even if the flag is deactivated.
incoming	Incoming calls may be received on the line.

Parameter Description of Tabs:

- **change line**
- **delete line**

Parameters	Description
Trunk	Displays the lines number.
Box/Slot/Port/Line	Displays the physical port of the line (Box/Slot/Port/Line).
Code	Display or entry of the seizure code
Route	Display or selection of the route that is assigned to the trunk (none or Trk. Grp 1 to Trk. Grp 12).
Ringing assignment per line	
Day call no.	Day service call number for incoming connections that are not DID-capable
Night call no.	Night service call number for incoming connections that are not DID-capable

Parameter Description of Tabs:

- **Change ISDN Flags**

Parameters	Description
Protocol: Description	Each protocol template entry comprises the items Interface, Protocol and Additional info: S0 Basic access 2B+D via S0 interface, BRI Basic access 2B+D via U2B1Q interface (USA), S2 Primary multiplex access 30B+D, T1 Primary multiplex access 23B+D (USA)
Logical/Physical	Logical or physical numbering of the channels
Slave B-channel neg: Master	Setting of master/slave within Layer 3. For connections, one side must be set as the slave and the other side as the master.
Up B-channel alloc: Down	Definition of B-channel numbering (must be the same in both systems)
S0 CHI format: S2M	Protocol format CHI, to be defined as S0 (short format) or S2M (long format)

Parameters	Description
Unsymmetric/Symmetric	Symmetrical or non-symmetrical use of L3 protocol elements
Automatic/Fixed	Auto-negotiation or fixed assignment of symmetry
1 CR length: 2	Protocol format call reference length
Alarm signaling	Use of alarm signaling in the layer 3 protocol
Protocol timers	Use of the layer 3 timer
PRI quickstart	Use of the PRI QuickStart procedure
IE_TNS	Use of the information element Transit Network Selection
IE_OSA	Use of the information element Open Service Access
CIDL	Use of call and link ID signaling in the network
Userside/Networkside	Layer 2 protocol setting. Mirrored setting required on the opposite side
Network/Subscriber	Layer 2 protocol setting. Mirrored setting required on the opposite side
PP/PMP	Point-to-point or point-to-multipoint setting, only relevant for S0
Permanent active	Layer 2 permanently active
Active TEI verify	Enables TEI check
Userside/Networkside	Layer 1 protocol setting. Mirrored setting required on the opposite side
PP/PMP	Layer 1 protocol setting. Same settings required on both sides
S Bus type: L	Short/long bus (ranges)
Permanent active	Layer 1 protocol setting. Same settings required on both sides
CRC4 check	Layer 1 protocol setting, only relevant for S2M, same setting required on both sides
CRC4 reporting	Layer 1 protocol setting, only relevant for S2M, same setting required on both sides

Parameter Description of Tabs:

- **Change B-Channel**

Parameters	Description
B channel	Displays the B channel number.
Outbound	Outgoing calls may be made on the B-channel.
Incoming	Incoming calls may be received on the B-channel.

Parameter Description of Tabs:

- **Change Direction**

Parameters	Description
Line	Displays the line number.
Outgoing	Outgoing calls may be made on the line.
Incoming	Incoming calls may be received on the line.

28.3.10.2 Trunks/Routing > Trunk group

Parameter Description of Tabs:

- **Change Route**

Parameters	Description
Route Name	Route name. The entered name replaces the default route number in the Routes list.
Seizure codes	The assignment codes for each route are entered here. The routing codes entered must be collision free, both mutually and within the communication system's entire call number plan. Use the Check button to test for collisions. The seizure code is the code that causes the switching system to provide a line to the station that dialed the code. Seizure codes only work if LCR has not been activated.
CO code (2nd. trunk code)	A second trunk code (CO code) is defined if the communication system is a subsystem of another communication system or is networked with several other communication systems. It is only relevant for networking routes (route type = PABX). In this case, the second trunk code is the seizure code for the main system. Within a network, the codes for the trunk seizure, the route seizure code(s) and the second CO code must be configured uniformly. The default in Germany is 0.
Gateway Location	
Country code	Displays the country code of the own gateway location. Set via Basic Settings/ Gateway/Gateway Locations
Local area code	Displays the local area code of the own gateway location. Set via Basic Settings/Gateway/Gateway Locations
PABX number	Displays the PABX number of the own gateway location. Set via Basic Settings/Gateway/Gateway Locations
System station number - incoming	
Country code	Used for digit analysis for incoming calls. Country code without leading zeros (e.g., 1 in the U.S., 49 in Germany)
Local area code	Used for digit analysis for incoming calls. Local area code without leading zeros (e.g., 89 for Munich)
PABX number	Used for digit analysis for incoming calls. PABX number (central company phone number, e.g., 777)

Parameters	Description
Location number	Used for digit analysis of public telephone numbers for outgoing connections. Checks the dialing information to determine whether the called destination number is located in the own system.
System station number - outgoing Info: Changes to outgoing PABX numbers must be coordinated with the network providers. (Clip no screening)	
Country code	Used for caller identification in outgoing calls. The country code without leading zeros (e.g., 1 in the U.S., 49 in Germany) is transmitted to the network. If no "PABX number outgoing" is entered, the "PABX number incoming" is automatically used.
Local area code	Used for caller identification in outgoing calls. The local area code specified here (without leading zeros, e.g., 89 for Munich) is transmitted to the network. If no "PABX number outgoing" is entered, the "PABX number incoming" is automatically used.
PABX number	Used for caller identification in outgoing calls. The PABX number specified here (central company phone number, e.g., 777) is transmitted to the network. If no "PABX number outgoing" is entered, the "PABX number incoming" is automatically used.
Suppress Stn. Call No.	Activating this flag suppresses the DID number in the caller ID.
Overflow route	
Overflow route	If all lines of the configured route are seized, an overflow to another route can be set. The overflow route applies only when LCR is disabled.
Digit transmission	
Digit transmission	The type of digit transmission is determined here for the selected route and is displayed as static (e.g., route table 6: en-bloc sending) text under Settings | Least Cost Routing | Dial plan after selecting the route table (see Route table drop-down list).
Digit transmission: Digit-by-digit	The digits are transmitted in sync with dialing.
Digit transmission: en-bloc sending	During en-block digit transmission (block dialing per route), the dialed digits are buffered by the communication system. Dialing only takes place when a timer has elapsed after the last digit has been dialed, when the end-of-dial code # has been entered or if an exact match in the dial rule is found. In the case of PRI in the USA block dialing to the central office is mandatory. LCR must be activated to be able to select en-bloc digit transmission. The type of digit transmission is automatically set to en-bloc digit transmission in the route table if at least one route of the LCR route table is configured with en-bloc digit transmission.
Mobile Extension Number (MEX)	

Parameters	Description
MEX Number	If the ITSP being used supports the "Mobile Extension (MEX)" feature, the MEX number (8 positions, with only digits) provided by the ITSP must be entered here. This feature can only be used only with an Internet telephony DID connection (SIP like ISDN). It is used integrate mobile phones/smartphones into the communication system. The user of the mobile phone can be reached via the One Number Service under a single phone number, which is also communicated to the other party. When a subscriber is conducting a call with his or her mobile phone, the office number of the subscriber is displayed to the other party, so the number of the subscriber's mobile phone remains unknown. In addition, other internal subscribers can check the presence status of such subscribers even if they are currently talking on their mobile phones.
Trusted External User	
Trusted External User	User that can be assigned to external collaboration platform such as MS Teams for making phone calls.

Parameter Description of Tabs:

- **Change Routing Parameters**

Parameters	Description
Routing flags	
Digit repetition on	When an outgoing route is seized with digit repetition activated, the routing code is sent before the call number. This only applies if LCR is deactivated (see Settings | Least Cost Routing).
Analysis of second dial tone / Trunk monitoring	Analysis of Second Dial Tone alerts the communication system to detect an additional dial tone. This feature is used with tandem communication system applications. This evaluation is country-dependent, e.g., in Belgium after 00 and in France after 16 or 19. This is not relevant in Germany. This only applies to network providers who send a second dial tone for international calls.
Intercept per direction	This flag is necessary for QSIG networking. When this flag is set, the communication system checks whether a diversion request has been received by the remote station, or whether the communication system has implemented forward switching to the central intercept position. The remote station receives a message which advises whether or not a diversion should be implemented for this call. If intercept is activated for a route, all calls forwarded to this route are intercepted at this intercept position. To implement this feature, day and night numbers must be configured for each route (see Ringing assignment per line). Furthermore, an intercept position should not be entered for the day/night service (see Intercept/Attendant).

Parameters	Description
Over. service 3.1 kHz audio	For all outgoing calls on ISDN, Over. service 3.1 kHz audio is the default setting. This is the standard transmission type for outgoing calls on an Integrated Services Digital Network (ISDN) line). A connection from the communication system to a digital CO with an analog modem must be identified as a data service. This flag should be set to avoid problems during FAX operation. In some cases, a network operator may not support the 3.1 kHz audio bearer service. This can cause the fax transmission to certain external telephone numbers to fail. One possible solution is to disable the **Over. service 3.1 kHz audio** flag.
Add direction prefix incoming	When this option is activated on system telephones with incoming seizure, the call number display is supplemented by the route code.
Add direction prefix outgoing	When this option is activated with outgoing seizure, the call number display is supplemented with the access code. Info: changing this parameter affects the caller identification and must therefore be coordinated with the network providers. (Clip no screening)
Call No. with international / national prefix	If this flag is enabled, the national or international code for the phone number (e.g., 02302…., 00492302...) must be added as a prefix for the ITSP. Default: enabled
Ring-back-tone to CO	If this flag is set, a 'Ring-back tone' will be sent to the ISDN central office on an incoming call. This is a special protocol handling required for the provider Global One and Sovintel.
Segmentation	This area defines the system behavior when sending ISDN messages in which the maximum Layer 2 user data length (260 bytes) is exceeded.
Segmentation: yes	The message to be sent is split into 260-byte segments and sent individually. The receiving communication system must support the segmentation and collect and arrange the individual segments into a message.
Segmentation: no	Segmentation is not needed, since the underlying Layer 2 can transport messages of any length.
Segmentation: Truncate Message	The message to be sent is truncated to less than 260 bytes by eliminating the less important portions (such as names, for example) and then sent.
Deactivate UUS per route	User-to-User Signaling (UUS) can be deactivated with this flag. This suppresses the transmission of the name and phone number of the A station in the UUI element (user-to-user information, UUI) for external call forwarding (FWD ext.). This flag must be manually deactivated for Telefonica.
Always use DSP	If this flag is set, a connection to the Internet telephony service provider is only possible via a DSP (digital signal processor). If this flag is not set, then there is a Direct Payload connection to the Internet telephony service provider. This flag must be set for the route of the OpenScape Voice network. This flag may not be set in the case of fax transmissions (T.38) via an external device (e.g., Mediatrix 4102).
Name in CO	This flag is configured for CO that support calling party name.

Parameters	Description
Analog trunk seizure	Here various times can be selected which determine when dialing begins when using analog dial-up lines (MSI). If no pause is set, the communication system waits until it recognizes a dial tone. Note for Brazil: When using DTMF signaling from analog terminals in conjunction with analog trunks and digit outpulsing after dial tone detection, there might be problems with the toll restriction when the country code is set to Brazil. In this case, the DTMF signals from the analog terminals go directly to the analog trunks ("1A procedure" is not used). Because of this, the DTMF signals which are dialed before the dial tone is received are lost. Consequently, for such cases, least cost routing (LCR) must be enabled for the dialing method and toll restriction to operate properly at the device.
Trunk call pause	The CO call pause determines the period of time that elapses before a call is recognized as being completed once the user has hung up. This option applies only to MSI lines. For a trunk call with, for example, 1 second on and 4 seconds off, a trunk call pause of 6 seconds should be configured. In some COs, however, a 10-second ring pause applies. In such cases, a trunk call pause of 13 seconds must be programmed. Otherwise, no call diversion can be implemented. In the United States, this cycle is two seconds on, two seconds off, for a total of six seconds. The six-second option is the default, so you will not need to make any changes here. Setting range: 2 to 13 seconds.
Type of Seizure	This field specifies the criteria that apply if the communication system needs to seize an outgoing line.
Type of seizure: cyclical	The communication system starts its cyclical search for a free line with the next line number based on the last outgoing line seized in this route.
Type of seizure: linear	The communication system always begins its search with the lowest line number assigned to this route.
Route type	There are two options for Route type. The type of route can be set either as CO (Central Office) or as PABX (Private Automatic Branch Exchange).
Route type: CO	Lines assigned to this route are subject to toll restriction. When LCR is active, the toll restriction is regulated by the Dial plan (COS column).
Route type: PABX	Toll restriction is only performed if there is a second CO code assigned to this route. When LCR is active, the toll restriction is regulated by the Dial plan (COS column). The route type also has a bearing on the default text of the route name (see Routes) as well as on the procedure used for recognizing the dial tone on MSI lines.

Parameters	Description
No. and type, outgoing	The administrator can configure the "PABX number, incoming" and "PABX number, outgoing" separately, divided into portions for the country code, local area code and PABX number (= connection number in the local network). This is needed for the implementation of the "CLIP no screening" feature. If no "PABX number outgoing" has been configured, the communication system will always use the data of the "PABX number incoming" setting. In the case of an incoming seizure on an ISDN line, the communication system truncates the PABX number (left-aligned) from the received phone number and interprets remaining portion as the Direct Inward Dialing number. For call number information to the PSTN, the communication system automatically inserts the PABX number (or the portion defined in the configuration) as the leading portion of the call number. This does not apply to dialing information (destination address). The call numbers of internal stations that are sent to the remote station can be composed as follows:
No. and type, outgoing: Unknown	only DID number (default setting)
No. and type, outgoing: PABX number	PABX number + DID number
No. and type, outgoing: Local area code	+ Local area code + PABX number + DID number
No. and type, outgoing: Country code	Country code + Local area code + PABX number + DID number
No. and type, outgoing: Internal	Only for networked systems: number prefixes may not be added for closed numbering plans. Call number prefixes are suppressed here.
Call number type	The settings in the "No. and type, outgoing" area also affect calls coming from an extension in a partner system (a networked node). Due to this setting, the caller's number that is received from the networked node and forwarded to the Central Office is extended for the outgoing route.
Call number type: Internal	In this case, only the internal call number is transmitted. If the destination is an external station, either no number is transmitted or only that of the Attendant Console. The internal call number can be displayed when the destination is an internal station on another node.
Call number type: Direct inward dialing	In this case, only the DID number is transmitted. The internal call number is not provided for display at internal destinations in other nodes. The call number information is sufficient for external destinations.
Call number type: Internal / DID	This setting is useful for networking purposes. Both the internal call number and the DID call number are transmitted to the destination station. If an internal station is called within the network, the internal call number of the caller can be displayed for this station. If the internal destination station has activated call forwarding to an external destination, for example, a DID number can also be transmitted in this case.
Rerouting	

Parameters	Description
Change route	When this flag is turned on, it is also possible to route D-channel information via other routes. This option enables alternative routing via other routes. The option may be activated only when the call number plan is unambiguous. (Closed numbering or unique seizure codes in a network. The system making the request must also support this.). If rerouting is implemented, rerouting with change route active must also be set for the corresponding route. This option is only available for CorNet NQ networking, and must be activated in the same way in both networked communication systems.
Route optimize active	To optimize use of the B-channel, call forwarding can be performed on the basis of the protocol in accordance with the specification "Call Forwarding/ Partial Rerouting". If partial rerouting is rejected, forward switching is used.
Route optimize active: No	When you select this option, Rerouting is deactivated. For call forwarding, the connection is always set up via two B-channels.
Rerouting active: If route is known	When you select this option, rerouting is only active if the route is known and a successful "handshake" procedure takes place between the two networked communication systems.
Route optimize active: Always	If the setup for the incoming call is coming in on the same route as the call forwarding destination route, the call will be rejected (call deflection feature is used) by the communication system if this option is activated. In case of networked systems this option Always must be activated in the same way in both networked communication systems.

Parameter Description of Tabs:

- **Special Parameter change**

Parameters	Description
Numbering plan Defines the Numbering Plan parameter in outgoing messages	
Called Party Number	System check = defined by the system; ISDN numbering plan, Private numbering plan, Unknown numbering plan = preset manually
All others	e.g., Calling Party No., Redirecting No, etc. System check = defined by the system. ISDN numbering plan, Private numbering plan, Unknown numbering plan = preset manually
Site	The Site (location) parameter determines how the Location parameter is set in the Q931 info element CAUSE and Progress Indicator. System check = defined by the system; alternatively, the setting "Private network and station" or "Always station" can be made manually.

Parameters	Description
COLP	If this flag is set, the number of the called party will be shown to the caller in the case of an external incoming CO connection. The calling party can see if the call has been forwarded or picked up by somebody else. This feature needs to be turned on by the central office as well. If the flag is set and an external incoming call is forwarded or intercepted, the updated call number is signaled to the CO in the connect message output by the communication system. If the COLP feature is activated in the CO, the updated call number is also displayed for the caller. Info: This flag does not affect the call number display for external outgoing connections.
Notify send	This message is used for the transmission of status information about the current connection. The message can be sent from the network as well as the subscriber side to notify the other party (network or subscriber) about an interrupted connection, for example, or that call forwarding is active. If the notify feature is not supported by the CO, the notify message can be suppressed by resetting this flag. If this option is activated, a "Notify" message is transmitted if a call is on hold or parked, for example. Notify send is only evaluated in the DSS1, NI1 and MCI protocols. In the SIP-Q, CorNet-NQ and QSIG the notification is always sent.
without CLIP	If this flag is set, the calling party information to the public network will be suppressed for outgoing calls on a BRI or PRI line. This flag can be activated or deactivated on a per route basis. In addition, the station has the option to suppress the called party information on a per call basis via an access code or the system telephone menu.
No SETUP ACK.	If this flag is set, the setup acknowledgment message from the communication system to the Central Office is suppressed. Relevant for special COs. Example: Fujitsu's Fetex150 COs.
no DIV.LEG-Info	If this flag is set, the standard diverting LEG information signal (call number of the redirecting party) is not sent to the CO. The DIV. LEG info should be suppressed if problems occur in the case of external call forwarding (CF ext.).
With sending complete	If this flag is set, the optional information "All digits sent" is output by the system once all dialed digits have been transmitted.
Internal call like external	If this flag is set, network-internal calls are acoustically signaled in the same way as external calls.
Without CCNR	If this flag is set, an incoming ISDN call with CCNR (Call Completion on No Reply) is signaled so that the system can accept a callback request. This means the caller can initiate a callback if the station does not reply. In some cases the message is not supported by the ISDN provider. In this case the switch must be activated to prevent the system from sending CCNR.

28.3.10.3 Trunks/Routing > QSIG Features

In a network consisting of several communication systems, any connection information that occurs (CDRC data) in the PBX satellite systems is sent to a fixed communication system in the network. For this purpose, the call number

of the destination system (call number of central recording system) to which the connection data is sent is configured in each communication system.

Parameter Description of Tabs::

- **Edit QSIG Features**

Parameters	Description
Own system data	
System number	This data identifies your own communication system in the network. This data applies to both central busy signaling and connection data routing. In a network consisting of several communication systems, each communication system has its own system number. If the communication system is networked with such communication systems, and you wish to use the QSIG features, the system numbers must also be administered here for compatibility reasons. Value range: 1 to 255
Group number	In the communication systems, subscribers can be classified into groups, which then receive a unique group number. This type of grouping does not exist in the communication system. However, for compatibility reasons, the group number must also be administered here. Value range: 1 to 40
Inter-system busy signaling	
System no. target system	This data defines a communication system where centralized busy signaling is used. This can be either the PABX or a PABX satellite system. System number of the communication system that is configured for central busy signaling. Value range: 1 to 255
Call no. target system	Call number of the communication system that is configured for central busy signaling. Enter the PABX number and not the station number in this field. The fact that no extension is entered for this PABX number must be taken into account in the LCR dial plan! Example: If the call number of the destination system is 999 the dial plan entry must be -999 (and not -999XXX and not -999Z).
Connection data - Routing	
Call no. target system	This data defines a communication system where centralized connection data recording takes place. This can be either the PABX or a PABX satellite system. Call number of the communication system that is set up as a central recording system (see also the note above for Call no. target system).

28.3.10.4 Trunks/Routing > Assign MSN

Parameter Description of Tabs::

- **Display MSN**
- **Edit MSN**

Parameters	Description
MSN	Display or entry of the MSN (point-to-multipoint call number).
Trunk	Displays the assignment of the trunk on which the MSN is active.

28.3.10.5 Trunks/Routing > ISDN Parameters

The reference clock (ISDN clock) synchronizes operations on CO trunks within a specific network or within the Central Office. Normally, the communication system automatically selects the trunk to be used as a reference clock for all of the communication systems within a given network or CO. However, if the reference clock line is missing or malfunctions, then you must configure one or more other trunks as the reference clock line.

The communication system chooses the trunk in the following order:

1) Allowed list
2) S_{2M} CO trunk
3) S_0 CO trunk
4) S_{2M} tie trunk (only slave configuration)
5) S_0 tie trunk

Parameter Description of Tabs:

- **ISDN Clock**

Parameters	Description
Index	The positions reflect the priorities 1-4 (for the Allowed list) and 1-16 (for the Denied list).
Allowed Lists	If the Allowed list contains entries, the automatic line selection of the communication system is overridden. The ISDN ports (max 4 possible) entered in the Allowed list are used first in the search for the reference clock line.
Denied Lists	The ISDN ports (max 16 possible) entered in the Denied list are skipped in the search for the reference clock line.

28.3.11 Classes of Service

The functions for the classes of service for CO trunks are grouped together under **Classes of Service**. They control subscriber access to external calls that may be subject to toll charges.

28.3.11.1 Classes of Service > Stations

Parameter Description of the Tab:

- **Show all stations**

Parameters	Description
Call No., **Call number**	Station number of the subscriber.
Name	Name of the subscriber.
Day	Selected COS group for the Day service.
Night	Selected COS group for the Night service.
Class of Service Group Day	Displays the COS group for the Day service. The selection you make refers to the **COS Day** table, where the COS group is linked to the actual classes of service.
Class of Service Group Night	Displays the COS group for the Night service. The selection you make refers to the **COS Night** table, where the COS group is linked to the actual classes of service.

NOTICE: Class of Service Groups texts are generated according to **Basic Configuration** wizard > **System Country Code**.

28.3.11.2 Classes of Service > Day: Class of Service Groups

Parameter Description of Tabs::

- **Edit Names**
- **Edit COS Group**
- **Day: Display COS Members**

Parameters	Description
Class of Service Group	Freely selected name for COS groups 1 to 15; assignment of CO call privileges per route (trunk) for day and night, respectively When configuring the stations, access to external call numbers can be restricted by assigning class of service groups.
Class of Service	Assignment of classes of service to the individual COS groups for day service. All restrictions are effective only for the lines for a route of the type CO.
Class of Service Group: Internal	The subscriber may only make internal calls. Default value: default in COS group 1
Class of Service Group: Outward-restricted	The subscriber may only answer (not make) external calls. Default value: default in COS group 2
Class of Service Group: Allowed list	The subscriber may only dial the external numbers defined in the Allowed list. Outward-restricted trunk access applies if no call number is entered. Default value: default in COS group 4
Class of Service Group: Denied list	The subscriber is not permitted to dial the external numbers defined in the Denied list. Unrestricted trunk access applies if no call number is entered. Default value: default in COS groups 3, 5, 6

Parameters	Description
Class of Service Group: Unrestricted	Subscribers can answer and set up incoming and outgoing external calls without restriction. Default value: default in COS groups 7 through 15
Display COS Members	Displays call numbers and names of the members of the selected COS group.

28.3.11.3 Classes of Service > Night: Class of Service Groups

Parameter Description of Tabs::

- **Edit Names**
- **Edit COS Group**
- **Night: Display COS Members**

Parameters	Description
Class of Service Group	Freely selected name for COS groups 1 to 15; assignment of CO call privileges per route (trunk) for day and night, respectively When configuring the stations, access to external call numbers can be restricted by assigning class of service groups.
Class of Service	Assignment of classes of service to the individual COS groups for night service. All restrictions are effective only for the lines for a route of the type CO.
Class of Service Group: Internal	The subscriber may only make internal calls. Default value: default in COS group 1
Class of Service Group: Outward-restricted	The subscriber may only answer (not make) external calls. Default value: default in COS group 2
Class of Service Group: Allowed list	The subscriber may only dial the external numbers defined in the Allowed list. Outward-restricted trunk access applies if no call number is entered. Default value: default in COS group 4
Class of Service Group: Denied list	The subscriber is not permitted to dial the external numbers defined in the Denied list. Unrestricted trunk access applies if no call number is entered. Default value: default in COS groups 3, 5, 6
Class of Service Group: Unrestricted	Subscribers can answer and set up incoming and outgoing external calls without restriction. Default value: default in COS groups 7 through 15
Display COS Members	Displays call numbers and names of the members of the selected COS group.

28.3.11.4 Classes of Service > Allowed Lists

Parameter Description of Tabs::

- **Display Speed Dials**

- **Add Call Number**

Parameters	Description
List 1-6	Display/Add/Edit/Delete an allowed number. The Allowed list contains the phone numbers that may be called by the subscriber. Up to 6 Allowed lists can be created. Your first Allowed list can have up to one hundred entries, and the remaining five lists can have a maximum of ten entries.
Phone number	Call numbers can contain up to 27 digits, which can include the numbers 0 through 9 and the symbols * and #. The complete telephone number does not need to be listed. To permit users to dial (toll free) 0800xxx numbers, for example, only 0800 needs to be entered here. Since these lists are only for outgoing external calls, it is not necessary to include the trunk seizure code with the numbers you enter.

28.3.11.5 Classes of Service > Denied Lists

Parameter Description of Tabs::

- **Display Speed Dials**
- **Add Call Number**
- **Edit Analysis Filter**

Parameters	Description
List 1-6	Display/Add/Edit/Delete a denied number. The Denied list contains the phone numbers that cannot be called by the subscriber. Up to six Denied lists can be created. The first Denied list can have up to fifty entries, while the remaining five lists can have a maximum of ten entries each.
Phone number	Call numbers can contain up to 27 digits, which can include the numbers 0 through 9 and the symbols * and #. The complete telephone number does not need to be listed. For example, to prohibit users from dialing (toll-based) 0900xxx numbers, you would only need to enter "0900" here. Entering a # sign at the start of a denied number prevents the toll restriction from being bypassed for system telephones when an analog CO line is to be seized using DTMF signaling or when switching to DTMF during the dialing. Since these lists are only for outgoing external calls, it is not necessary to include the CO access code with the numbers you enter.
Edit Analysis Filter You can use exception filters for any Denied list to define which digits should not be compared with the corresponding Denied list. The communication system excludes the set range of digits before the digit analysis.	
From digit ... **To digit**	The analysis filter is active in this numeric range (1-25) within the phone number.
Character	By prohibiting the characters * and #, subscribers are prevented from entering these characters to bypass the toll restriction.

28.3.11.6 Classes of Service > Blacklist

Parameter Description of Tabs:

- **Display List**
- **Add Call Number**

Parameters	Description
Call number	Call numbers can contain up to 25 digits, which can include the numbers 0 through 9 and the character +. The ’+’ character refers to the international prefix that is configured in the system and must be entered in the first position. The first character of each entry can be ’+’ or any digit. The telephone numbers are numerically sorted in the Blacklist. Blacklist entries must be entered in international (e.g., 004989) or in canonical international format (e.g., +4989).
Block Anonymous calls	Enabling this flag blocks the calls with no originator number or with existing originator number but restricted presentation.
Blacklist feature on	Enabling this flag blocks the added call numbers. Blacklist feature is based only n calling party number (call originator) given by the provider.

28.3.11.7 Classes of Service > Night Service

Parameter Description of the Tab:

- **Edit night service**

Parameters	Description
Authorized station for night service	If you want particular stations to have the ability to switch the communication system to night mode, you must enter these stations to the list of stations in the Authorized Station for Night Service list. A maximum of 5 stations can be entered. Default value: 100
Station	List of all stations present in the communication system.
Authorized station	List of authorized stations that can enable night mode.
Add >>	Adds the selected station to the authorized stations list

28.3.11.8 Classes of Service > CON Group Assignment

Parameter Description of Tabs::

- **Edit Group Assignment**
- **Trunk to Group**
- **Group Speed Dial Range**

Parameters	Description
CON Group Assignment	Assignment of a CON group (1-64) to a subscriber. You can assign a CON group to individual stations in the communication system via the CON Group Assignment. When coding the connection matrix, you can then access these stations and define which stations can reach which other stations. All stations are assigned to CON group 1 by default. This provides all stations with unrestricted access to all other stations. Value range: 1 - 64
Trunk to Group	Assignment of a trunk to the CON group. You can assign a CON group to individual lines in the communication system via the CON Group Assignment. When coding the connection matrix, you can then access these groups and define which subscribers can access which lines. All CO trunks are assigned to CON group 1 by default. All stations thus have unrestricted access to all trunks (both inbound and outbound). Value range: 1 - 64
Group Speed Dial Range	Every CON group is assigned a range of speed dials (SSD). If a user selects a speed dialing system number, the system determines whether or not this user is authorized to select that speed dialing system number by determining the associated ITR group. The number is dialed if this speed dialing system number belongs to the range of speed dialing system numbers assigned to the relevant CON group. An error message is issued if the speed dialing system number does not belong to the assigned group. The speed-dial number ranges can overlap in the CON group. Individual speed dialing system numbers may not be entered in the ITR groups and multiple speed dialing system number groups may not be entered in an ITR group. For example, the following are allowed: CON 1: 0-99; CON 2: 50-150; CON 3: 200-500. And the following are not allowed: CON 1: 0, 5, 10; CON 2: 50-100, 300-500. Value range: 0-7999

28.3.11.9 Classes of Service > CON Matrix

Parameter Description of Tabs::

- **Edit the CON Matrix**

Parameters	Description
CON matrix	If you want to selectively edit one connection method between two CON groups, click in the field at the intersection point of these CON groups in the CON matrix. Click repeatedly in the field to release or block the connection methods in one direction, the other direction, or both directions. To use the connection matrix, you must first assign each station to a group via Group assignment. By default all stations and all trunks are in Group 1. Since Group 1 is coded with unlimited access, by default, every station has access to every other station and to all trunks.

Parameters	Description
Grid	Note that the matrix shows one list of groups vertically across the top and another list of groups horizontally down the left-hand side. At each conjunction there is a box. The type of arrow in this box indicates the relationship of the two groups to one another. An empty field means that no connection is possible. A connection matrix with no arrows results in a totally disabled communication system.
Block all	The CON matrix suppresses traffic between stations and trunks within the same group (subsystem) and between groups.
Release all	The CON matrix allows traffic between stations and trunks within the same group (subsystem) and between groups.
Group-internal only	The CON matrix allows traffic only between stations and trunks within the same group (subsystem).

28.3.11.10 Classes of Service > Autom. night service

Parameter Description of Tabs::

- **Display all days**
- **Edit day**

Parameters	Description
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Special Day	Day which is configured via the schedule. The schedule covers the entire week (Monday through Sunday) as well as special days. Special days are holidays or special days such as company holidays.
Zone	The schedule for a day can be split into up to 4 zones (time intervals). These zones can be defined sequentially and without gaps, that is, the end time of the first interval may be identical to the start time of the second interval, for example. However, an interval cannot have the same start and end times. The minimum length of an interval is 15 minutes. Value range: 1-4
Begins	Start time for the zone. If the first interval for a day begins at 0.00 hours, then the start time must be entered as 00:00.
End	End time for the zone. If the last interval for a day ends at 24.00 hours (12 p.m.), the end time must be entered as 23:59 (11:59).
Night call no.	Night phone number for the zone. If no call number is entered for the night call number, night service per line is activated in the system. The destinations for this are set under **Lines/networking** > **change line** > **Ringing assignment per line**. The timers entered via the automatic night service apply for all trunks.
OK	The zone will be created.
Delete	The defined zone will be deleted.

Parameters	Description
Copy Service	You can copy the zones set up to one or more other days by selecting the day you want, to the special day by selecting the respective flag, all to all by selecting **Check all**. When you hit **Apply**, the zone settings in the days you have selected will be overwritten with the zones set up in the current day.

28.3.11.11 Classes of Service > Special Days

Parameter Description of the Tab:

- **Edit Special Days**

Parameters	Description
Day	When you select a date in the calendar, this is automatically entered here.
Name	Name for this special day (e.g., Whit Monday)

28.3.12 Auxiliary Equipment

The functions for auxiliary equipment such as Music on Hold (MoH), configuring Announcements or for connecting an entrance telephone as a Door Opener at the system ports (trunks), are grouped together under **Auxiliary Equipment**.

28.3.12.1 Auxiliary Equipment > Music On Hold

Parameter Description of Tabs:

- **Edit Music on Hold**

Parameters	Description
Type of MOH	Type of MOH parameter allows you to choose among three possible options. The music for this feature can be supplied internally or externally.
Type of MOH: No Music On Hold	If this option is selected, the Music on Hold feature will be deactivated completely. This does not apply when an external call is transferred by a transfer before answer; the caller then hears the ring tone.
Type of MOH: MOH without ringing tone	If this option is selected, in the case of an unmasked transfer, the caller will hear Music on Hold while the transfer takes place, as well as while the call is being transferred by the transferring party and the external connection is ringing at the transferred destination.

Parameters	Description
Type of MOH: MOH with ringing tone	If this option is selected, in the case of an unmasked transfer, the caller will hear Music on Hold while the transfer takes place. As soon as the call is transferred through by the transferring party and the external connection is ringing at the transferred destination, the caller will hear a ring tone. The MOH with ringing tone option should always be set in a network system in order to provide the customer with a uniform environment. |If the caller is reaching the system through Internet Telephony Service Provider(ITSP), this option will not apply and the caller will hear Music On Hold during transfer.

Access and Type activation via Manager E.

The input format for Music On Hold is a wave file with PCM and 16 bits. Supported sample rates are 8, 22.05, 24, 32, 40, 44.1 and 48 kHz in mono or stereo. The preferred format is PCM, 16 bits, 8kHz, mono. The recommendation is to use the preferred input format and limit the length of the wave files to about 2 min. It is possible to set one MOH for day and one for night. A reset is required.

28.3.12.2 Auxiliary Equipment > PhoneMail

Parameter Description of Tabs:

- **Edit PhoneMail**

Parameters	Description
Callback Access phonemail	Set the **Call number** and **Name** of the device.
Live recording device	Set the **Call number** of the device.

28.3.12.3 Auxiliary Equipment > Announcements

Parameter Description of Tabs:

- **Edit Announcements**

Parameters	Description
WAVE File	Here you can select the WAVE (.wav) for a specific announcement (see Configuration > Announcements > Load to Gateway).

Parameters	Description
Access	The connection is defined via Access. Here you can select the port (SLA analog or EVM) to which this device is connected. **INFO:** Analog ports that are set up as announcement ports must be assigned the value "Answer machine", under **Expert Mode** > **Telephony Server** > **Station** > **Analog Stations** > **Edit** > **Extension Type**, as described in Station Parameters. External destinations can be used to address announcement devices in another system node. To do this, the announcement device is identified as external. The call number of an announcement port in another system node is entered here. **INFO:** This equipment list refers to the **Announcement** setting, under **Expert Mode** > **Telephony Server** > **Incoming calls** > **UCD** > **Edit UCD Group Parameters**, as described in Incoming calls > UCD. If you select **External destination** the following two fields appear: • **Route** (trunk groups) • **Call number** (device)

Parameters	Description
Type	You can select one of the following type of announcements from the drop-down menu: • **None**: Announcement equipment is not connected. • **Announcement**: Enables the connection of only one external announcement device via SLA ports or EVM cards. The announcement provided by the activated announcement device must have a fixed beginning and end. This device should not forward the call after the end of the announcement (a switching destination should not be entered). The corresponding announcement device port is entered under **Access**). Equivalent to **start/stop** for external destination devices. • **Music On Hold**: An announcement or music is repeated continuously. Queued calls can also be connected while the music or announcement is being played. Connection is possible either via SLA ports or EVM cards. The corresponding announcement device port is entered under **Access**. Equivalent to **continuous** for external destination devices. • **Internal Music**: Activates the system-internal music-on-hold in the communication system. For this option, **None** should be entered under **Access**. External MOH (Manager E configuration) is heard if defined as a destination in the communication system. Entries under **Access** have no effect on either variant. • **Media PC**: This setting is predefined. The media PC or controlling application controls whether the caller hears the announcement from the beginning or is connected to an on-going announcement. • **Announcement Player**: The announcement player is an internal software program that is available together with the UC Booster functionality (UC Booster Card or UC Booster Server). **NOTICE:** The announcement player functionality is only available in UC Suite mode.
Mode	You can select one of the two following options: • **start/stop**: single playback • **continuous**: continuous playback

NOTICE: The **Music on Hold / Announcements** wizard can also be used to configure **Announcements**. For more information see How to Configure Announcements.

28.3.12.4 Auxiliary Equipment > Door Opener

Parameter Description of Tabs:

- **Edit Door Opener**

Parameters	Description
Station	Selection of the phone number / connection port of the entrance telephone. The Station port type must be P.O.T or No Port.

Parameters	Description
Destination	Selection of the phone number / connection port of the entrance telephone ring destination. A station number or a group number can be specified as the ring destination at which a special ring is signaled when the doorbell button is pressed. The call is signaled in accordance with the call forwarding algorithms defined in "Settings - Incoming calls".
Door opener	Activates the door opener function. By setting this flag, a door opener connected at the TFE-S can be activated for the stations.
DTMF	Setting this flag enables the door opener to be activated remotely with a DTMF transmitter.
FWD	Setting this flag enables external forwarding of the entrance telephone ring destination.

28.3.12.5 Auxiliary Equipment > SmartVM

Parameter Description of Tabs:

- **Edit SmartVM Mailboxes**

Parameters	Description
Mailbox call no.	Input of the mailbox call numbers. A mailbox is identified by means of the mailbox call number. If a mailbox is to be assigned to a station, the mailbox must have the same call number as the station.
Name	Displays the mailbox name. The name corresponds to the name of the subscriber (if available). In the case of a group, the group name is displayed.
Greeting	Selects the greeting. The usability of the items offered will depend on the selected phone menu (TUI). With the OSO TUI, only Greeting 1 is supported for standard mailboxes.
Greeting: **Greeting 1-4**	The selection of Greetings 1-4 depends on the type of the mailbox: Standard mailbox: Greeting 1 or 2 (only Greeting 1 with OSO TUI) Attendant mailbox: Greeting 1, 2, 3 or 4
Greeting: **Day/Night**	The greeting depends on the Day/Night mode: Day - Greeting 1 / Night - Greeting 2
Greeting: **Type of Call**	Only for standard mailbox: Greeting depends on the status of the subscriber: Call not accepted - Greeting 1 / Busy - Greeting 2
Greeting: **None**	No greeting is played. However, the mailbox remains active, e.g., to forward the call to the intercept position.

Parameters	Description
Recording	If this flag is enabled, the mailbox is a standard mailbox. It can then no longer be an Attendant mailbox. If the flag is disabled (default), the mailbox does not have the option of recording a message. The subscriber can activate the recording when checking his or her voicemail box for the first time. This ensures that no messages can be recorded before the mailbox has been activated by the user. Default: enabled
AutoAttendant	If this flag is enabled, the mailbox is an Attendant mailbox (AutoAttendant). It can then no longer be a standard mailbox. A maximum of 100 mailboxes can be configured as Attendant mailboxes. When a standard mailbox is converted to an Attendant mailbox, all existing messages of the mailbox are deleted. Default: disabled
Password Reset	If this flag is enabled, the password of the mailbox is reset to `123456`. The subscriber must change the password at the next access to his or her mailbox. Default: disabled

Parameter Description of Tabs:

- **Edit SmartVM Parameters**

Parameters	Description
General parameters	
Max. mailbox no. length	Maximum length of voicemail box call number. Value range: 2 - 16 positions; default value: 3 positions
Max. message length (min)	Maximum length of the recording time for a message. Range of values: 1 or 2 minutes; default value: 2 minutes
Call number length delimitation	For outgoing connections that are initiated by the SmartVM (AutoAttendant suffix dialing and AutoAttendant speed dialing), only call numbers up to the specified length can be dialed. In cases where longer call numbers have been configured, no connection is established. By default, the call number length restriction corresponds to the (internal) call number length of the mailbox, so only internal dialing is allowed. Value range: 2 to 30, default value: 3
General fax intercept	Entry of the fax intercept destination to which the SmartVM should normally send incoming faxes. If no fax intercept destination is specified, incoming faxes will be rejected. Value range: max. 16 digits
Standard lang.	Selects the language of the user prompts. Applies to all mailboxes. If user prompts in the desired language are not available, the language is set to UK English (enuk).
Telephone User Interface	Selects the phone menu structure of the voicemail box (Telephone User Interface, TUI). The selection applies to all voicemail boxes.
Telephone User Interface (TUI): **SmartVM**	SmartVM TUI, EVM TUI (default).

Parameters	Description
Telephone User Interface (TUI): **OSO**	OSO TUI, similar to the UC Suite TUI.
Order of Date Announcement	Only visible with SmartVM TUI: Setting of the announcement sequence for message, recording date and number of the caller (if known).
Order of Date Announcement: **Date After Message**	Only visible with SmartVM TUI: Message - Recording date - Number of the caller (if known).
Order of Date Announcement: **Date Before Message**	Only visible with SmartVM TUI: Recording Date - Number of the Caller (if known) - Message. The following applies to messages from internal subscribers: Name of the internal subscriber (if available) -- Recording date -- Number of the caller (if known) -- Message.
Amount of Messages per Mailbox	Maximum number of messages for a mailbox. Value range: 0 to 100, default value: 30
EVM Deactivation	If this flag is enabled, the SmartVM is disabled. Default: disabled
Allow callback from VM to know number only	When external UserA calls UserB, UserB has call forward to his voice mail, external UserA leaves a voice message, UserB call the SmartVM, enter his password and while listens to the message dials the digit ’8’. By dialing this number there is a callback to UserB. If this flag is enabled callback occurs if the the number of userB belongs to the known numbers. Known numbers are the Mobile phone number and the Home/external phone number of the profile details of User Management(Applications-UC Smart-User Management) Default: enabled
AA VP Behavior Setting for whether the AutoAttendant should automatically play announcements for certain cases.	
VP Before Transfer	If this flag is enabled, the following announcement is played for "VP Before Transfer": "Please wait, you are being connected..." Default: disabled
VP Transfer Result	If this flag is enabled, one of the following prompts is played for "VP Transfer Result": "The station number does not exist." "The station is busy." "The station is not responding." Default: enabled

Parameters	Description
VP Intercept	If this flag is enabled, one of the following announcements is played for "VP Intercept": "You are being connected with the operator. Please wait." "You are being connected with the mailbox of the subscriber." "Please wait, you are being connected..." Default: enabled
VP Before Release	If this flag is enabled, one of the following prompts is played for "VP Before Release": "Please call later." "Thank you. Goodbye." "The mailbox number is not valid." Default: enabled

Parameter Description of Tabs:

- **Edit Automatic Attendant Parameters**

Parameters	Description
Call number	Call number of the AutoAttendant (default: 352).
Intercept after announcem.	If this flag is enabled, the call is intercepted to the intercept position (e.g., the attendant console) after the greeting. No speed-dialing destination can be dialed during the announcement of the greeting. Default: disabled
no suffix-dialing	If this flag is activated, the caller can only be redirected to other destinations by the dialing of speed-dial destinations. The caller cannot dial any multi-digit call number. Default: disabled

Parameter Description of Tabs:

- **Edit Speed Dial/Intercept Dest. Day**
- **Edit Speed Dial/Intercept Dest. Night**
- **Edit Speed Dial/Intercept Dest. 3**
- **Edit Speed Dial/Intercept Dest. 4**

Parameters	Description
Select	Selection of an internal subscriber (1st. half of the list) or a voicemail box (2nd. half of the list) as a speed dial destination or intercept position.
Action	Displays the 10 possible speed dial destinations and the intercept position.
Call number	Call number of the selected subscriber or the selected voicemail box.
Name	Name of the selected subscriber or the selected voicemail box.
Type	Selects the type of the call number.

Parameters	Description
Type: **Call number**	In this case, the selected subscriber is called with the assigned speed dial number.
Type: **Mailbox**	In this case, the selected voicemail box is called with the assigned speed dial number.

28.3.13 Payload

The functions for displaying and configuring port types and protocols are grouped together under **Payload**.

28.3.13.1 Payload > Devices

Parameter Description of Tabs::

- **Display Global Device Settings**
- **Reset Device Settings to Factory Settings**

Parameters	Description
Global Gateway of Type G.711	Devices is the collective name for stations, features, and functions that require channels. The information displayed includes the codec type of the global gateway, the maximum number of licensed B channels available, and the maximum number of LAN clients on a channel for music on hold (calls above this number are not put through).
Max. No. of B Channels Supported by Hardware	
No. of LAN Clients per MoH Channel	

Resetting the device settings requires a restart of the communication system.

28.3.13.2 Payload > Media Stream Control (MSC)

Parameter Description of Tabs::

- **Edit MSC Jitter Parameters**

Parameters	Description
	The Media Stream Control (MSC) monitors and administers the media streams that are routed via the communication system. It provides for the transfer of media data between networks via gateways(TDM/IP).
Traffic Statistics (SNMP Only)	Required for access to the data of the per-call statistics of the system via SNMP.
RTCP Packet Generation Interval (sec)	Report interval in seconds for RTCP packets (Real-time Transport Control Protocol). This interval is used for the negotiation and compliance of Quality of Service (QoS) parameters through the periodic exchange of control messages between senders and receivers. Value range: 5 to 10, default value: 5

Parameter Description of Tabs::

- **Reset MSC Settings to Factory Defaults**

Parameters	Description
Reset MSC Settings to Factory Defaults	Restore all original settings of the MSC.

28.3.13.3 Payload > HW Modules

Manage the DSP modules of the communication system

Parameter Description of Tabs:

- **Display All HW Modules**
- **Edit DSP Settings**
- **Edit DSP Jitter Settings**

Parameters	Description
HW Type	Displays the DSPs (Digital Signal Processors) used in the communication system. Possible options are: • **Onboard** = Integrated DSP of the mainboard • **OCCB X-1** = DSP of an OCCB subboard (OCCB1 or OCCB3)
Firmware version	Current firmware version of each individual DSP
API Version	Current API (Application Programming Interface) version of each individual DSP
General	
IP Address	IP address of the DSP module (can be changed if the IP address is already used). ***Note:*** The last octet of IP address cannot be .1 (xxx.xxx.xxx.1)
Port	Port number of the DSP module
Status display	Used to detect the availability of DSPs Default value: Status messages
Echo Canceller	Enabling this flag suppresses the echo effect in voice transmissions. Default value: Enabled
DTMF Outband Signaling	When this flag is activated, DTMF signals are transmitted in a separate signaling channel (outband transmission). Default value: Disabled
Fax Parameter	
Number of Redundancy Packets	Defines the number of redundancy packets: the higher the value, the lower the risk of packet loss during fax transmission. Higher values, however, also require a higher bandwidth. Default value: 2

Parameters	Description
Maximum Network Jitter (hex msec)	Defines the maximum network jitter in milliseconds: the higher the value, the greater the possible round-trip delay of data packets in networks. Only hexadecimal values consisting of the digits 0 to 9 and A to F are allowed. Avoid making any changes to this parameter. Default value: 00C8
Fax/Modem Tone Detection Timeout (s)	Defines the time in seconds for the detection of fax tones during calls: this ensures that the T.38 fax protocol is used. After the preset time has elapsed, no more fax tones are detected. A value of 0 means that fax tone detection is enabled for the entire duration of the connection. Default value: 0
DSP Jitter	
Jitter Buffer Type	Definition of the Jitter buffer type Default value: Adaptive
Jitter Buffer Type: Static	The average delay of the jitter buffer always remains the same.
Jitter Buffer Type: Adaptive	The jitter buffer aligns with the average delay when receiving data. It attempts to keep the delay as low as possible while keeping data packet loss to a minimum.
Average Delay for Voice (ms)	Defines the time in milliseconds during which an IP packet should be held in the jitter buffer in the case of IP-based voice transmission. ***INFO:*** In the case of the **Jitter Buffer Type Adaptive**, the value defined here is only a start value. Default value: 40
Maximum Delay for Voice (ms)	Defines the maximum delay for voice in milliseconds **Jitter Buffer Type Static**: Enter the maximum number of milliseconds permitted for a delay before the jitter buffer intervenes in the data stream when receiving IP packets as part of a voice transmission. The recommended value for the static jitter buffer is 80 for most environments. **Jitter Buffer Type Adaptive**: Enter the maximum number of milliseconds for the average delay for voice. Outgoing packets are lost if the actual delay measured is greater. The recommended value for the adaptive jitter buffer is 120 for most environments. ***Note:*** This value must always be greater than the value specified in the "Average Delay for Voice (ms)" field. Default value: 120
Minimum Delay for Voice (ms)	Defines the minimum delay for voice in milliseconds **Jitter Buffer Type Adaptive**: Enter the minimum number of milliseconds permitted for the average delay for voice. The average delay is always greater than or equal to this value. Default value: 20

Parameters	Description
Packet Loss / Delay Preference	Defines the ratio between packet loss and propagation delays for data packets **Jitter Buffer Type Adaptive**: Specify a value between 0 and 8 depending on what seems more acceptable in the event of large propagation delays - loss of packets or even greater delays. A value of 0 means minimal packet loss and greater propagation delays. A value of 8 means minimal propagation delays and a higher risk of packet loss. The recommended value for most environments is 4. Default value: 4
Average Delay for Data (msec)	Defines the average delay for data in milliseconds Enter the average number of milliseconds a data packet should be held in the jitter buffer for data transmissions. The recommended value for most environments is 60. Default value: 60
Maximum Delay for Data (msec)	Defines the maximum delay for data in milliseconds Enter the maximum number of milliseconds permitted for a delay before the jitter buffer intervenes when receiving IP packets as part of a data transmission. The recommended value for most environments is 200. ***INFO:*** Higher values (from about 2000) have no effect. As soon as a packet has entered the buffer, it will leave the buffer again. Although values under 100 msec are possible, they are not recommended in practice. Default value: 200

28.3.14 Statistics

The functions for displaying statistics are grouped together under **Statistics**.

28.3.14.1 Statistics > Gateway Statics > Mainboard > Device Statistics

Parameter Description of Tabs::

- **Display SCN Statistics**
- **Display LAN Statistics**

Parameters	Description
Device Type	Displays the existing LAN and SCN (Switched Circuit Network) components.
No. of Currently Used Resources	Displays the currently allocated resources of a component (configured and used channels).
Total	Displays the sum of the currently allocated resources.
auto refresh	The display is automatically updated every 60 seconds.
Seconds until next automatic refresh	Displays a countdown timer, starting at 60 seconds.

Parameters	Description
DDS1 Subscriber	As soon as a mobile telephone moves into the area of a different radio switching location (“current-location cordless board”), an extension connection is switched using a DSS1 connection initiated by the cordless board. So, DSS1 Subscriber refers to the number or mobile phones or DSS1 connections established in the switch.
HFA / IP Networking Voice	This SCN component, shows the number of DSP channels that are occupied, when gateway calls are established.
Music on Hold	When the DMC interworking feature is active in an IP network, gateway connections are set up over DMC channels. From the user’s perspective, a DMC channel is a gateway channel that provides a gateway connection.
SIU	Signalling Unit (SIU) reserves a DSP channel used to detect or generate system tones, such as DTMF tones
DMC	Displays a countdown timer, starting at 60 seconds.
H.323 (RTP)	Displays the used resources in case of a voice call.
T.38 Fax	Displays the used resources in case of a fax connection.
PPP	Displays the used resources in case of a Point-to-Point connection.

28.3.14.2 Statistics > Gateway Statistics > Mainboard > MSC Statistics

Parameter Description of Tabs::

- **Display Overall Statistics**

  MSC statistics are statistics of the media stream, which is implemented on digital signal processors between IP and TDM (Media Stream Control). The MSC overall statistics offer an overview of the statistical data for all registered calls. It provides information on the sent and unsent RTP/TCP packets, the packets received and not received, and the number of bytes sent and received.

Parameter Description of Tabs::

- **Display Per-Call Statistics**

  The MSC Per-Call Statistics show the connection data and parameters used for each connection involving conversions using digital signal processors in tabular form. It is used for error analysis by experts.

28.3.14.3 Statistics > SNMP Statistics

Parameter Description of Tabs:

- **Display Statistics Table**
- **Display Statistics**

Parameters	Description
ifTable Statistics	SNMP statistics for individual interfaces (if = interface) of the communication system (e.g., Ethernet interfaces).

Parameters	Description
IP Statistics	Details and errors associated with IP routing
TCP Statistics	Details and errors associated with the TCP protocol
UDP Statistics	Details and errors associated with the UDP protocol

28.3.14.4 Statistics > Telephony Statistics > System Texts

Parameter Description of Tabs:

- **Display System Texts**

Parameters	Description
Available languages	Displays the telephone user interface languages available in the communication system

28.3.14.5 Statistics > Telephony Statistics > UCD Agents

Parameter Description of Tabs:

- **Display UCD Agents**

Parameters	Description
Count UCD agents	
Total	Total number of UCD agents logged into the communication system
Available	Number of available UCD agents
UCD agent state	
Phone number	Call number of the UCD agent
Name	Name of the UCD agent
ID	ID of the UCD agent
UCD group	UCD group to which the UCD agent is assigned.
Status	Status of the UCD agent

28.3.14.6 Statistics > Telephony Statistics > Trunk Status

Parameter Description of Tabs:

- **Display Trunk Status**

Parameters	Description
Date	Date of status query or date of last status change for trunk

Parameters	Description
Time	Time of status query or time of last status change for trunk
Slot/Port	Displays the board, the slot and the interface (port) or the LAN Interface
Route	Displays the route name, to get a better hint to which ITSP a line belongs.
Trunk Number	Trunk code
Comment	Trunk status (the most recent status of the trunk is displayed.) Possible line statuses: • **Idle** (line idle) • **Alerting** (call is pending) • **Connected to:** (connected to the displayed phone number) • **Line shutdown** • **Line failure**

28.3.14.7 Statistics > Telephony Statistics > Forwarding

Parameter Description of Tabs:

- **Display Forwarding**

Parameters	Description
Call forwarding	
Status	Status of call forwarding: • **Off** (no call forwarding rules active) • When call forwarding has been enabled, the call forwarding type and destination are displayed.
Forwarding destination from	Indicates whether the called party is the forwarding destination of a call forwarded by another subscriber. The call number and name of the forwarding subscriber are displayed.
Ringing group on	
Stations included	The number and name of the stations included in the ringing group
Connection of	Indicates whether the station is the ringing group destination of another station. The call number and name of the primary station are displayed.

28.3.14.8 Statistics > Telephony Statistics > Stations

Parameter Description of Tabs:

- **Display Station Parameters**
- **Display Activated Features**

Parameters	Description
Phone number	Station number

Parameters	Description
Name	Name of the station
Direct inward dialing	DID number of the station
Device type	Type of phone (e.g., OpenStage 60)
Clip/Lin	Location Identification Number LIN For U.S. and Canada only: the enhanced E911 emergency service transmits geographical information on the caller in addition to the phone number when an emergency call is dispatched. Every station number with a valid DID number must be assigned a LIN.
Access	For analog and $U_{P0/E}$ phones: the board, the slot and the port number are displayed. Additional information which is only displayed for $U_{P0/E}$ phones: master or slave. For IP phones: the LAN interface, the type and the number are displayed
Parameters	
Extension Type	Station type, such as Standard or Fax Default value: Standard
Language	Language setting of the telephone
Call signaling internal	Call type for the signaling of internal calls Default value: Ring type 1
Call signaling external	Call type for the signaling of external calls Default value: Ring type 1
Class of Service (LCR)	Class of Service for Least Cost Routing (LCR) Default value: 15
Licence Type	License type of the station
Features	
Do Not Disturb	Status of the Do not Disturb feature Default value: off
Answer text	Status of the Answer text feature Default value: off
Lock code	Status of the Lock code feature Default value: off
Suppress calling ID	Status of the Suppress calling ID feature Default value: off
Ringing group on	Status of the Ringing group on feature Default value: off

Parameters	Description
Disable incoming ringing	Status of the Ringer cutoff feature Default value: off
Out of Hunt group/Group ringing	Status of the Group Call/Hunt Group feature Default value: off
Call waiting tone	Status of the Silent camp-on (call waiting tone) feature Default value: off
Direct answering	Status of the Direct answering feature Default value: off
Call waiting terminating	Status of the Call waiting terminating feature Default value: off
Call forwarding after timeout	Status of the Call forwarding after timeout feature Default value: off
FWD	Status of the Call Forwarding (CF) feature Default value: off

28.4 Applications

Functions for configuring the Application Server for Unified Communications and Web Services are grouped together under **Applications**.

28.4.1 Application Selection

The functions for selecting the Unified Communications solution are grouped under **Application Selection**.

28.4.1.1 Application Selection

Parameter Description of Tabs:

- **Application Selection**

Parameters	Description
Select application packages	Choice of application packages with UC Smart or with UC Suite. For the application package with UC Suite on the OpenScape Business UC Booster Server, the IP address of the UC Booster Server (IP address of the Linux server) is also required.
Application Selection	Display of the supported components, depending on the selected application package, including the IP address of the server used.

28.4.2 Active Directory Integration Service

The relevant functions for integration of the Acrive Directory are grouped under **Active Directory Integration Service**.

28.4.2.1 Active Directory Integration Service

Parameter Description of Tabs:

- **Active Directory Integration Service**

Parameters	Description
Sync Type	The values that sync type can have are the following: • **empty** No synchronization of the user with the Active Directory service is done. • **did** Automatic synchronization of the user with Active Directory. The DID number is used as a synchronization key. • **forced** Manual synchronization of the user with an Active Directory user. With forced synchronization, it is possible to synchronize an Active Directory user with multiple OpenScape Business users. • **mulap_member** The automatically synchronized user is a member of a mulap group.
Search	The empty fields on top of the screen can be used for searching for a specific user when the number of users is too big to fit in one screen. In fields **First Name**, **Last Name**, **Display Name**, and **DID**, a "starts with" search is conducted. In field **Active Directory User** a "contains" search is conducted. Search is initiated after pressing the button **Search**.
Edit	You can use this button to configure the synchronization of the specified user. The available actions when you select **Edit** are the following buttons that appear.
Save Data	You can select a specific AD user and force the synchronization with the specific OpenScape Business user. You can synchronize in this way different DID numbers to the same AD user.
Reset	Try to sync the OpenScape Business user with any Active Directory user. This action can be used, for example, if the user synchronization is stopped.
Do not Sync	Stop the synchronization of the specified OpenScape Business user. Already synchronized data for the user are not removed, but further synchronization with AD is discontinued.

28.4.3 UC Smart

The relevant functions for unified communications are grouped under **UC Smart**.

28.4.3.1 UC Smart > Basic Settings

Parameter Description of Tabs:

- **Basic Settings**

Parameters	Description
Enable / Disable UC Smart	
Active	UC Smart and UC Suite cannot be active simultaneously. (Additional parameters appear after activation)
Enable / Disable CloudService	
Active	This flag controls the state of the CloudService functionality. Note that enabling the CloudService feature will cause a WebServices restart.
Access Rules	
HTTP	UC Smart clients basically access the system with encryption using HTTPS (recommended) or without encryption using HTTP (not recommended). The selection is made in the application itself. The authorization for one or both of these protocols is granted here.
HTTPS	
Password Policy	
Force user to choose secure password	Password policy for UC Smart clients. The default password must be changed at the first login, and the new password must comply with policy selected here (see exclamation mark button). The password is stored in the client; otherwise, it is requested whenever the client is started.
Save login data for devices	The login data is additionally stored in the phone.
System-wide initial UC Smart password	A system-wide initial password affects all configured UC Smart users who have never logged into UC Smart or who have not changed their initial password. Each affected user must then assign a custom password. ***INFO***: The initial assignment of a system-wide UC Smart password presents a security risk, especially if the individual users do not promptly assign a personal password. Alternatively, the assignment of individual initial passwords for each user is recommended.
Office Hours	
Start Time	You can configure Office hours by selecting two values from the Start Time and End Time drop-down lists accordingly. Default office hours are between 08:00 a.m. and 20:00 p.m.
End Time	
Presence	
Hide sick status	You can hide the 'Sick' presence status option from UC clients users.

28.4.3.2 UC Smart > User Management

Parameter Description of Tabs:

- **User Management**

Parameters	Description
User	List of all existing users; the selected user must obtain a UC User license
Settings	
Users	Displays the internal phone number of the user.
Name	Displays the name of the user.
Password	The password of the user of the UC Smart client can be set here.
Language	Language of UC Smart Assistant
The user must assign a new password	(display only)
UC Smart Assistant access	Authorization for access to UC Smart Assistant by the user
Configured as Mobility stations	(display only)
Voicemail licence	(display only)
Associated Services	(display only)
Profile details	
Mobile phone number	Mobile phone number of the subscriber in canonical format (e.g., `+ 49 173 1234567`).
Private/External phone number	Additional phone number of the subscriber in canonical format (e.g., `+ 49 89 987654321`).
E-mail Address	E-mail address of the subscriber.
Voicemail to e-mail	Enable/disable the e-mail notification when a new voice message is received.
Presence visibility	Setting that determines whether the presence status is visible to both internal and external subscribers or just to internal subscribers or not visible to any subscribers.
Licence information	Display of licenses available in the system for each application

28.4.3.3 UC Smart > Status

Parameter Description of Tabs:

- **Status**

Parameters	Description
Application Server	Displays the status of the integrated UC Smart application server.
Active Sessions	Displays the number of active connections per UC Smart client.

28.4.4 OpenScape Business, UC Suite

Under **OpenScape Business UC Suite** you will find a group of unified communications functions such as conferencing, departments and groups, configuring the external directory, holiday and other schedules, the Contact Center and the server settings for the UC Suite.

28.4.4.1 OpenScape Business, UC Suite

Parameters	Description
OpenScape Business UC Suite	Configuration of the UC Suite, including the myPortal, myAgent, myAttendant and myReports clients, voice and fax messages and conferencing.

28.4.4.2 OpenScape Business, UC Suite > User Directory

If you want to change your first and last name, this has to be done by the administrator. Otherwise, the changes will not be kept after a synchronization happens. A synchronization happens when the system restarts or any settings are changed by the administrator.

A subscriber who is member of a MULAP group is not displayed in the user directory. If the subscriber is member of a hunt group, he/she is displayed in the user directory.

Parameters	Description
Search	Search for a UC Suite user.
Symbol for presence status	The administrator can change the presence status for every user and set their return date and time in Day-Month-Year (DD/MM/YY) and 24-hour (HH:MM) format respectively. A grey figure is currently not logged into the UC Suite. **NOTICE:** Every member of a hunt group is considered as system directory user and is displayed in greyed out color.
Edit	Edit settings of the selected UC Suite user. **NOTICE:** Due to a known browser compatibility issue, the layout of the **Edit User** window may differ when using Firefox. The layout is consistent with IE/Chrome/Edge.

Parameters	Description
Reset User	Reset the settings of a user to default values. All the user's voicemail messages, personal greetings for the voicemail box, journal entries, scheduled conferences, e-mails and faxes are deleted in the process. **NOTICE:** In this case, the default password is set to 4 characters (1234).
Unlock User	Users who have been locked (e.g., after multiple incorrect password entries) can be unlocked here; displayed through the lock symbol. The administrator can be notified about the lock by the system via e-mail.
Personal Details	Personal data of the user
Personal Details: My Personal Details	Login Name, Password, Last Name, Extension, First Name, VoiceMail Number, Fax Number, Assistant Number, Email, Department, Mobile Number, External Number 1/2, Home Number (in canonical format, e.g., +49 89 700798765). The password is valid for UC Suite clients.
Personal Details: My Picture	Is automatically scaled Supported file formats: BMP, JPG/JPEG/JFIFI, PNG. Maximum file size: 10MB
Personal Details: User Level	Can be set only by the administrator for contact centers: if the agent is to be permanently available, select the **Permanently available agent** check box. The agent will then remain available for calls, faxes and e-mails even when he or she does not accept a call, fax or e-mail. When a user is configured as an agent, the rights of the agent are defined by selecting the appropriate class of service for that agent (i.e., the authorization level as an Agent, Supervisor or Administrator), from the **Level** drop-down list . An agent with the authorization level of a Supervisor or Administrator has elevated privileges.
My Preferences	User-specific settings of the client.
My Preferences: Appearance	Skin colors of the user interface; language of the user interface; usage or not of classic traypop.
My Preferences: Notifications	Settings for screen pops.
My Preferences: Presence	Settings for presence status.
My Preferences: Outlook Connectivity	Generate Calendar Appointments: automatically transfer presence status into Outlook calendar; Calendar Integration: control of presence status through Outlook/iCal appointments (the first keyword in the subject line controls the presence)
My Preferences: Hot Keys	Define hotkeys for call functions.

Parameters	Description
My Preferences: Miscellaneous	Auto-reset presence status to "Office" after end of appointment, enable recording of client logs, define method of transfer, retention period for journal entries (maximum value is 30 days), programming function keys of the phone, enable live search and include LDAP contacts in directories' live search, specify an answer message.
Call Rules	Rules for incoming calls
Call Rules: Forwarding Destinations	Define forwarding destinations for each presence status (status-based call forwarding)
Call Rules: Rules Engine	Define complex call rules, based on the presence status (rule-based call forwarding)
Communications	Handling of user-specific messages
Communications: VoiceMail Settings	Option of recording of voice messages in each presence status; setting the voicemail language Default value: disabled
Communications: VM Notification	Notification service for new voicemail - see My Personal Details e-mail address. Prerequisite: the mail server and own e-mail address is configured under Service Center > E-mail Forwarding. "Outbound" generates a user outcall to the specified phone number (in canonical format). For the SMS phone number, see My Personal Details. For SMS templates, see the section in Templates.
Communications: Fax Notification	Notification service for new fax messages - see My Personal Details e-mail address. Prerequisite: the mail server and own e-mail address is configured under Service Center > E-mail Forwarding. "Outbound" generates a user outcall to the specified phone number (in canonical format) either within business hours only or 24 hours a day. For the SMS phone number, see My Personal Details. For SMS templates, see the section in Templates.
Communications: Missed Call Notifications	Notification service for new missed calls - see My Personal Details e-mail address. Prerequisite: the mail server and own e-mail address is configured under Service Center > E-mail Forwarding.
VoiceMail Profiles	Profile for personal AutoAttendant
Busy, No answer, Meeting, Sick, Break, Out of Office, Vacation, Lunch, Home	A caller can be redirected to a forwarding destination by post-dialing digit from 0 through 9 (suffix dialing) or can leave a message. As a prerequisite, an announcement is required for each presence status.
Profiles: Skip Dynamic Greeting	The automatic announcement of the presence status is skipped; instead, a caller hears only the announcement of the name and then the Personal AutoAttendant
Sensitivity	Settings to preserve the confidentiality
Sensitivity: Security and Access	Release of voicemails for myAttendant; checking the voicemail box from the own phone without a password; allow other users to see who you are talking to and copy your BLF layout.
Sensitivity: Presence Visibility	Set the visibility of the own presence status for internal users

Parameters	Description
Sensitivity: VoiceMail Presence	Announcement of your presence status to external callers. Input of internal phone numbers to be blocked, with the optional use of wildcards.
myAttendant	Display only for subscribers who are licensed for myAttendant
myAttendant: LAN Messages	Text modules for instant messages from myAttendant, free input, selection in the chat window of the client
myAttendant: DIDs	Input of DID numbers; if myAttendant is to be used for multiple companies, a "For" window can be displayed
myAttendant: Communications	Input of an internal number for call forwarding in an emergency or on non-acceptance (Unattended Forward) by myAttendant (for the U.S.)

28.4.4.3 OpenScape Business, UC Suite > Departments

Parameter Description of Tabs:

- **Departments**

Parameters	Description
Department Name	Departments classify subscribers in the internal directory into groups based on their organizational affiliation. This enables the an automatic assignment of users to departments in myAttendant, for example.
Hunt Group	(internal numbering with no further significance)
Add	Add a new department.
Edit	Edit a selected department.
Remove	Remove the selected departments.

28.4.4.4 OpenScape Business, UC Suite > Groups

A voicemail group enables a specific group of subscribers to access voicemails. When a call is placed to the call number of a voicemail group, the call is sent directly to the voicemail (i.e., the voicemail box) of the group and not to the group members.

A fax group (fax box group) enables a specific group of subscribers to access fax messages. The fax box of the group is reached directly via the call number of the fax group.

Favorites groups allow you to create groups with contacts and assign them to the users.

Parameter Description of Tabs:

- **VoiceMail Groups**
- **Fax group**
- **Favorite Groups**

Table 64:

Parameters	Description
VoiceMail groups	
Edit	Edit the selected voicemail group
Remove	Remove the selected voicemail groups
VoiceMail groups	Name of the voicemail group
Pilot	Call number of the voicemail group
Type	Type of voicemail group
# Users	Number of members in the voicemail group
# Message	Number of new voicemails for the voicemail group
Users	Members of the voicemail group
Fax group	
Edit	Edit the selected fax group
Fax Group	Name of the fax group
Pilot	Call number of the fax group
# Users	Number of members in the fax group
# Faxes	Number of new fax messages for the fax group
Multi-Users	If it is a fax group, **Yes** is displayed. Otherwise **No** is displayed.
Favorite Groups	
Add	Add a new favourite group
Edit	Edit the selected favourite group
Remove	Remove the selected favourite groups
Group Name	Name of the favorite group
Number of Contacts	Number of the contacts that have been added to the group
Editable	Select if the user can edit or not the favorite group.

28.4.4.5 OpenScape Business UC Suite > Templates

Parameter Description of Tabs:

- **SMS Provider**

Parameters	Description
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.
Edit	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.
Remove	Remove the selected Template.
Set To Default	Set the selected Template as default.

28.4.4.6 OpenScape Business UC Suite > External Directory

Parameter Description of Tabs:

- **External directory**

Parameters	Description
Add	Manual addition of individual contacts to the external directory. The characters must match the UTF-8 format
Edit	Edit a selected contact of the external directory.
Remove	Remove the selected contacts of the external directory

Parameter Description of Tabs:

- **Import External Directory**

Parameters	Description
Import from	Choose whether the import of contacts information will be done from a local file or from a public Windows folder.
File Upload	Click **Choose File** to select the file to be uploaded to the system.
Public Windows Folder	Enter the **Filename**, **Username**, **Domain**, **Password** of the public windows folder to be uploaded to the system and click **Test** to test it.
Options	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.

Parameter Description of Tabs:

- **Export External Directory**

Parameters	Description
Export to	Choose where the exported file will be saved, locally or in a public Windows folder.

Parameters	Description
Public Windows Folder	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 > External Providers Config

Parameter Description of Tabs:

- **LDAP Providers**

Parameters	Description
Add / Edit / Remove	Add, edit or remove the access data of the LDAP server.
Name	Name for this external offline directory
Server / Server address	DNS name or IP address of the LDAP server.
Port	Port number of the external LDAP server
Username	Username for accessing the remote LDAP server.
Password	Password for accessing the remote Exchange server.
LDAP Base Distinguished Name	LDAP base distinguished name, e.g., dc=example-for-a-domain, dc=net.
TLS	Enable the use of only secure connections to the LDAP server.
Title, **First Name**, **Last Name**, **Business 1**, **Business 2**, **Home Ph**, **Mobile**, **Company**, **Company Ph.**, **Postal Address**, **State or Province Name**, **Country Name**, **Postcode**, **E-mail**, **Pager**, **Facsimile Phone Number** and **City**	During the configuration of an external offline directory, the administrator can adapt the mapping of fields to the names of the used LDAP server. Deleted fields are ignored when searching for names via phone numbers. The search always occurs with the last 4 positions of the phone number preceded by a wildcard. You can deactivate the search for names via phone numbers for incoming calls. Enter the corresponding field name of the LDAP server in each case. **NOTICE:** LDAP field mapping depends on the corresponding field name by the use of external LDAP server.

Parameter Description of Tabs:

- **Exchange PST**

Parameters	Description
Add / Edit / Remove	Add, edit or remove the access data of the Exchange Server. In a Microsoft environment, the Active Directory Server (ADS) or the Exchange Server also serves as the LDAP server.
Name	Name of this external offline directory.
Auth Method	Authentication method to use for accessing the remote Exchange server. You can choose between **Basic** and **OAuth 2.0**.

Parameters	Description
Server / Server address	DNS name or IP address of the Exchange server.
Username	Username for accessing the remote Exchange server.
Password	Password for accessing the remote Exchange server. Visible only if the selected authentication method is **Basic**.
Tenant ID, **Application ID**, **Client Secret**, **Scope**	**Tenant ID**, **Application ID** and **Client Secret** corresponding to the application that has been registered in Azure AD for Exchange Directory Integration. They can be obtained from your Azure AD administrator. **Scope** the application requires (optional). Default value: https://outlook.office365.com/.default Visible only if the selected authentication method is **OAuth 2.0**.

Parameter Description of Tabs:

- **Exchange Calendar Integration**

Parameters	Description
Exchange Calendar Integration	The calendar integration is used for the automatic creation of Outlook appointments under Windows when the user is absent. If the Outlook appointments are not to be stored in the local PST file of the user, but on the Exchange server instead, the requisite access data must be entered here.
Enable Exchange calendar integration	Enable the Exchange calendar integration
Auth Method	Authentication method to use for accessing the remote Exchange server. You can choose between **Basic** and **OAuth 2.0**.
Server	Information on the usage of the various Microsoft Exchange servers can be found in the Unify Experts wiki at: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.
Username	Username for accessing the remote Exchange server.
Password	Password for accessing the remote Exchange server. Visible only if the selected authentication method is **Basic**.
Tenant ID, **Application ID**, **Client Secret**, **Scope**	**Tenant ID**, **Application ID** and **Client Secret** corresponding to the application that has been registered in Azure AD for Exchange Calendar Integration. They can be obtained from your Azure AD administrator. **Scope** the application requires (optional). Visible only if the selected authentication method is **OAuth 2.0**.

28.4.4.8 OpenScape Business UC Suite > Contact Center

Parameter Description of Tabs:

- **Schedule**
- **Queue**

- **Grade of Service**
- **VIP Caller Priorities**
- **VIP Call List**
- **Preferred Agents**
- **Contact Center Breaks**
- **Simple Wrapup**
- **Multiple Wrapup**
- **Queue Bindings**

Schedule

A schedule is used to define how incoming calls are to be handled on certain days and at specific times. For each queue, a schedule can be defined with rules (Call Control Vectors or CCVs) to determine how incoming calls are to be handled on specific dates and at specific times. A schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. The rules determine how incoming calls for a queue are to be handled during the time period to which the schedule applies. Rules apply only to calls and not to faxes and e-mails.

For detailed information on configuring schedules, see Configuration Procedure

Parameters	Description
Schedule	Schedule Name
Queue	Name of the queue to which the schedule is assigned.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Schedule	
Schedule Name	Schedule Name
Default CCV	Displays the default rule for the schedule, which applies to a queue 24 hours a day and 365 days in the year when assigned. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV).
Queues	
Queue Name	Name of the queue to which this schedule is assigned.
Queue Active	Indicates whether the queue is active or inactive.
Exceptions	
CCV	Name of the exception rule (exception CCV). Exception rules define how incoming calls received during certain exceptional times (break, weekend, holiday, vacation, etc.) are to be handled. Holiday schedules have precedence over the other schedules and rules of a queue.
Description	Descriptive text for the exception rule
Type	Type of the exception rule

Parameters	Description
Start Date	Date for the beginning of the exception rule
End Date	Date for the end of the exception rule
Start Time	Time for the beginning of the exception control
End Time	Time for the end of the exception rule
Occurs	The frequency the exception rule is scheduled

Queue

Queues are the basis of the Contact Center. Calls, faxes and e-mails for a queue can be handled, depending on the skill levels of agents, the priorities and waiting periods. Announcements can be played for waiting callers.

For detailed information on configuring queues, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
General Settings	
Queue Name	Queue Name
Queue Active	Definition of the queue status
Queue Active: Inactive	The queue is not active.
Queue Active: Active	The queue is active.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Phone Switch	Displays the CSP entry
Schedule	Displays the assigned schedule
Queue Alarm Count	Alarm threshold number If the number of calls waiting in the queue exceeds the number specified here, the queue symbol for the agent changes from green to orange. Default value: 0 calls
Queue Alarm Time	Alarm threshold time in seconds If the waiting time for a queued call specified here is exceeds the time specified here, the corresponding item in the list of Contact Center calls for the agents changes to red. Default value: 0 seconds

Parameters	Description
Missed Call Timeout	Missed call timeout in seconds If a call is not answered after the time specified here, it is forwarded to the next free agent. Default value: 10 seconds
Abandoned Call Threshold	Threshold value for abandoned calls in seconds The time specified here determines whether or not an abandoned call is included in the statistics. Calls abandoned after the specified time has elapsed are included in the statistics. Default value: 0 seconds
Screen Pop Enabled	When this flag is activated, a screen pop to display and enter customer data appears in myAgent for incoming calls. Screen pops are needed to accept and execute callbacks and to accept faxes and e-mails. Default value: Disabled **NOTICE:** Notifications option via **myAgent** > **Setup** > **Notifications** > **Pop up application on inbound calls** are overridden by the activation of the screen pop via **WBM** > **Expert Mode** > **OpenScape Business UC Suite** > **Contact Center** > **Queue** > **General Settings** > **Screen Pop Enabled**.
Wrapup Mode	Definition of the wrapup mode
Wrapup Mode: No Wrapup	No wrapup reasons can be defined for the queue.
Wrapup Mode: Simple Wrapup	One or more wrapup reasons can be defined for the queue.
Wrapup Mode: Multiple Wrapup	One or more wrapup reasons can be defined for the queue and then classified into groups and subgroups.
Screenpop Time Out	Screenpop timeout in seconds If the value is set to 0, there will be no screenpop time out. If the field is left empty, the previous assigned value is used. Default value: 20 seconds
Priorities	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.
Queue depth mode	Definition of the queue depth mode
Queue depth mode: Static	In case that the Queue Depth mode is set to Static, WLS and Queue Depth Size can be configured.
Queue depth mode: None	In case that Queue Depth is set to None the WLS Parameter can be configured and affects also the UCD configuration but parameter Queue Depth Size cannot be set

Parameters	Description
Queue Pilots	
Inbound Fax Pilots	Phone numbers (pilots) for incoming faxes Faxes to these phone numbers will then be added to the queue and treated as incoming calls.
Inbound E-mail Service	E-mail addresses for incoming e-mails E-mails sent to these addresses are placed in the queue and treated like incoming calls.
Add	Add a new Inbound Email Service
Edit	Edit a selected Inbound Email Service
Remove	Remove the selected Inbound Email Service
Auth Method	Authentication method to use for accessing the inbound email service You can choose between **Basic** and **OAuth 2.0**.
Server	DNS name or IP address of the inbound email service
Port	Port number of the inbound email service
Username	Username for accessing the inbound email service
Password	Password for accessing the inbound email service Editable only if the selected authentication method is **Basic**.
Uses SSL connections	Enable or disable the use of SSL connections according to the configuration of the Inbound Email Service
Tenant ID, **Application ID**, **Client Secret**, **Scope**	**Tenant ID**, **Application ID** and **Client Secret** corresponding to the application that has been registered in Azure AD for E-mail Queues. They can be obtained from your Azure AD administrator. **Scope** the application requires (optional). Default value: https://outlook.office365.com/.default Visible only if the selected authentication method is **OAuth 2.0**.
Miscellaneous	
Return Email Address	Sender E-mail address for sent emails The e-mail address specified here is displayed to the recipient when an e-mail is sent by an agent.
Intelligent Call Routing	When this flag is activated, incoming calls are automatically forwarded to the agent with whom the caller was last connected, As a prerequisite, no preferred agent must have been defined for the caller. Default value: Disabled

Grade of Service

The Grade of Service can be used to assess the response rate of the queue. This is achieved by comparing the waiting time for callers in the queue with target values, which can be specified individually for each queue here.

For each call to an appropriate queue, the service level is determined after the call and committed to the database. The Grade of Service can be evaluated by agents with the authorization level of a Supervisor or Administrator by using the myAgent application.

For detailed information on defining target values for the Grade of Service, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Grade of Service	The horizontal axis shows the waiting time in the queue in intervals of 10 seconds, and the vertical axis shows the target value for the Grade Of Service as percentage values. The red dots specify the target values for the quality of switching in the queue. Quality assessments can then be made by comparing these target values with the actual waiting times for callers in the queue.

VIP Caller Priorities

The VIP Caller Priority can be defined individually for each queue in order to specify whether callers included in the VIP Call List should be given preferential treatment.

The values for the VIP Caller Priority can be defined freely, depending on the waiting time for callers in a queue. This determines the level of preference for VIP callers as opposed to normal callers.

When a VIP caller activates an agent callback (by recording a voicemail with a callback request), the agent callback is retained in the queue instead of the VIP caller. The VIP caller priority is not applied here.

For detailed information on defining the VIP caller priority, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
VIP Caller Priority	The horizontal axis shows the waiting time in the queue in intervals of 30 seconds, and the vertical axis shows the priority of normal callers who are not registered in the VIP call list directory. The red dots define the priority of normal callers as opposed to VIP callers.

VIP Call List

Callers who have already been registered in the communication system (external directory) can be added to the VIP call list. In addition, call number patterns can be entered. A call number pattern consists of a specific sequence

of digits and a wildcard (placeholder). It can thus be used to transfer all employees of a company to the VIP call list, for example.

For detailed information on configuring the VIP call list, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
VIP Call List	Displays the callers and call number patterns included in the VIP call list. You can Add, edit or remove callers and call number patterns from the VIP Call List. The further right the scroll bar is for a caller or call number pattern, the higher the priority over the other callers or call number patterns contained in the VIP call list.

Preferred Agents

Every caller can be assigned one or more preferred agents of a queue. In such cases, the communication system first tries to switch the caller and his callback requests through to a preferred agent. If multiple preferred agents have been specified, a priority (sequence) can be defined to determine the order in which these agents are connected.

If no preferred agent is available, the call is forwarded to any available agent.

For details on defining preferred agents, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Preferred Agents	Displays the preferred agents for each caller indicated in the customer list. You can add, remove and change the priority of an agent. If multiple preferred agents were defined for a caller, the list position shows the priority over the other preferred agents. The higher an agent is positioned in the list, the higher the priority of that agent.
Display only customers who have agent associations	When this flag is activated, only the callers for whom at least one preferred agent was defined are displayed in the customer list Default value: Disabled

Contact Center Breaks

In order to allow every agent the chance to take a defined break, Contact Center breaks of different lengths can be defined. Contact Center breaks

are available system-wide and can be selected by an agent via myAgent as required.

For details on defining Contact Center breaks, see Configuration Procedure

Parameters	Description
Add	Add a new Contanct Center Break
Edit	Edit a selected Contanct Center Break
Remove	Remove the selected Contanct Center Break
Name	Name of the Contact Center break
Duration	Duration of the Contact Center break in minutes
Active	Indicates whether the Contact Center break is active or inactive.

Simple Wrapup

One or more wrapup reasons can be defined here for queues with the wrapup mode "Simple Wrapup".

Wrapup reasons can be used to assign incoming calls to specific categories (orders, complaints, service, etc.). The assignment is made by an agent after completing the call (during the work time) by entering the appropriate wrapup reason using myAgent.

For details on defining wrap-up reasons, see Configuration Procedure

Parameters	Description
Add	Add a new simple wrapup
Edit	Edit a selected simple wrapup
Remove	Remove the selected simple wrapup
Queue	Name of the queue for which simple wrapup was configured.
Description	Descriptive text for the wrapup reason.

Multiple Wrapup

For queues with the wrapup mode "Multiple Wrapup", one or more wrapup reasons can be defined here and then classified into groups and subgroups.

Wrapup reasons can be used to assign incoming calls to specific categories (orders, complaints, service, etc.). The assignment is made by an agent after completing the call (during the work time) by entering the appropriate wrapup reason using myAgent.

For details on defining wrap-up reasons, see Configuration Procedure

Parameters	Description
Queue	Name of the queue that was configured for multiple wrapup. The groups and subgroups already defined for this queue are displayed.
Description	Descriptive text for the wrapup reason.

Queue Bindings

Queues bindings are used to assign agents to one or more queues.

For details on assigning agents to queues, see Configuration Procedure

Parameters	Description
Queue	Queue Name
Queue Active	Indicates whether the queue is active or inactive.
Hunt Group	Hunt group identifier of the UCD group, which was set up during the basic configuration of the Contact Center.
Agent Assignment (Binding)	
Extension	Display of the user's extension number
Name	Display of the user's name.
Agent	Agent assigned to the queue.
Type	Agent Type The following options are possible: • Primary Agent: The agent receives calls regardless of the load on the queue. • Overflow Agent: The agent receives calls only when the queue overflows.
Skill Level	Displays the skill level in percent The skill level controls the distribution of calls to agents in a queue. Agents with higher skill levels are given preference during the call distribution. In cases where all agents have the same skill level, the longest idle agent receives the call.
Enable agent callback	When this flag is activated, the agent receives callback requests in the form of voice messages.
Work Time	Automatic work time in seconds
Overflow after seconds in queue	Only for Overflow Agent: Overflow time in seconds When the overflow time has elapsed, a call is routed to an overflow agent.
Overflow after calls in queue	Only for Overflow Agent: Number of calls Calls that exceed this maximum number are routed to an overflow agent.

28.4.4.9 OpenScape Business UC Suite > Schedules

Parameter Description of Tabs:

- **Edit/Add**

Parameters	Description
Auto Attendant	Configure the AutoAttendant function for the UC Suite (Company AutoAttendant)

Parameters	Description
Schedule	Schedule Name
Queue	Name of the queue to which the schedule is assigned.
Hunt Group	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)
Schedule Name	The schedule can be saved under a user-defined name. It is recommended that you enter a meaningful name here.
Default CCV	The schedule, in turn, must have at least one rule (called a Call Control Vector or CCV) assigned to it. Rules determine how incoming calls are to be handled during a specific time period. Rules apply only to calls and not to faxes and e-mails. Rules are created with the graphical rule editor (CCV Editor) by combining predefined CCV objects. Several predefined, standardized templates are available; these can be changed as desired and adapted to specific needs.
Queues	It is recommended to activate only one queue per schedule (set only one check mark).
Queue Name	The queue can be saved under a user-defined name. It is recommended that you enter a meaningful name here.
Queue Active	The queue can be enabled or disabled.
Schedule	Select the associated schedule.
Pilot	Call number of the associated virtual port in the communication system.
Exceptions	A schedule with an assigned default rule applies to a queue 24 hours a day, 365 days a year. If different rules are to applied at certain times (breaks, weekends, holidays, vacations, etc.), these can be assigned to the schedule as exception rules (Exception CCV). This means that you can define how incoming calls are to be handled during the holiday schedule, for example. Holiday schedules have precedence over the other schedules and rules.
CCV	Selection of the exception rule (exception CCV).
Description	Enter a description for the exception schedule
Type	Within the time range of one or more weekdays / Freely definable within the time date range / Holiday schedules for a specific date range
Start Date	Beginning of the exception (date)
End Date	End of the exception (date)
Start Time	Beginning of the exception (time)
End Time	End of the exception (time)
(Weekday)	The exception will apply to one or more weekdays
Occurs	The frequency the exception is scheduled

28.4.4.10 OpenScape Business UC Suite > File Upload

Parameter Description of Tabs:

- **Audio File Manager**

Parameters	Description
Upload Destination	Application for which the new announcement is used
Upload Destination: Auto Attendant	Announcements for the Automatic Attendant
Upload Destination: Profiles	Announcements for some or all users of UC Suite
Upload Destination: Voicemail Greeting	Voicemail announcements for all or individual users of UC Suite The maximum recording length of Voicemail Greeting is limited to 1 minute.
Upload Destination: VM Group Greeting	Greeting for a group voicemail box
no key for: uploader	The announcement is available for upload as a PCM file with the following properties: 8 kHz, 16 bit, mono. The maximum length for the audio file name is 30 characters.
Recorder	The announcement is recorded via the telephone of an extension
Wave File	
Download	Downloaded announcements.
Delete	Delete downloaded announcements.
Rename	Rename downloaded announcements.
Recorder	
File name	Species the file name of the announcement to be recorded.
Extension	Selects the phone with which the announcement is to be recorded.
Make Call	Calls to the phone with which the announcement is to be recorded.
Play	Plays back the recorded announcement.
Record	Starts recording the announcement.

Parameter Description of Tabs:

- **Central Fax Cover Page Upload**

Parameters	Description
Central Fax Cover Page Upload	
Ocp file	Fax cover page available as ocp file
Name	The name of the central fax cover page
Description	A description for central fax cover page
Upload	Upload the central fax cover page file

Parameters	Description
Edit	Edit the selected central fax cover page file
Remove	Remove the selected central fax cover page file
Set To Default	Set the selected central fax cover page file as default
File name	Species the file name of the announcement to be uploaded.
Creation Date	The creation date of the central fax cover page file

28.4.4.11 OpenScape Business UC Suite > Conferencing

Parameter Description of Tabs:

- **Conferencing**

Parameters	Description
Name	Name of the conference (assigned by the user)
Owner	Name of the user of who initiated the conference
Next Scheduled	Next scheduled start time
Active	
# Members	Number of conference participants, including conference controller
Display	Participants of the selected conference
Delete	Delete the selected conferences

28.4.4.12 OpenScape Business UC Suite > Site List

Parameter Description of Tabs:

- **Site List**

Parameters	Description
Site Name	Sites in the networked communication system (see Basic Settings > Gateway Properties)
Site Address	IP address of UC Card Booster, UC Booster Server or the communication system
Site Port	Server Port
Site IP Trunks	Site IP trunks, if available
Online Status	Connection status of the communication system at the site

28.4.4.13 OpenScape Business UC Suite > Server

Parameter Description of Tabs:

- **General Settings**
- **Live Record**
- **Logging**
- **Notifications**
- **Maintenance**
- **VoiceMail**
- **Contact Card Mapping**

Parameters	Description
Office Hours	
Start Time	Beginning of the daily office hours (business hours) Setting for the presence status of the UC clients Default value: 07:00 **NOTICE:** The entered value must be in 24-hour (HH:MM) format.
End Time	End of the daily office hours (business hours) Setting for the presence status of the UC clients Default value: 19:00 **NOTICE:** The entered value must be in 24-hour (HH:MM) format.
Length of Password	
Lengths	Length of the password for the UC clients. Minimum value is 6. ***NOTE:*** Changing the length of the password resets the passwords for all users. Default value: 6
Call number of intercept position	
Target Number	Call number of intercept position ***INFO:*** Enter the call number of the intercept position configured in the communication system.
Instant Message	
Disable instant messaging	When this flag is activated, the sending of instant messages is impossible. Default value: Disabled
Analog Extensions	

Parameters	Description
Analog User Mode	Defines how analog stations are displayed in the internal directory Default value: Show All
Analog User Mode: Show All	All analog stations are displayed in the internal directory
Analog User Mode : Show named only	Only analog stations with a name are displayed in the internal directory.
Analog User Mode: Not shown	No analog station is displayed in the internal directory.
Extension	
Max. internal length	Maximum number of digits for internal call numbers Default value: Max length of all internal extensions.
Min. external length	Minimum number of digits for external call numbers Default value: Max internal extension length +1. If it is less than 4, it is set to 4.
Transfer	
Normal Auto Attendant SST	When this flag is activated, the call will be transferred, regardless of whether the destination is free, busy or unavailable. Default value: Enabled
Journal	
Allow deleting of journal entries	This flag allows or prohibit the possibility for a user to delete a journal entry or not.
Hide "Open" calls in Journal	Hides the **Open** button under Journal.
Fax Format	
Use PDF as fax format	If the flag is activated, the received fax can be saved in a PDF format, otherwise the received fax is saved in tiff format.
Directory Server	
Slow External Provider	This flag improves the response time of the right mouse click to an e-mail. Also, when it is activated, searches of contacts are executed only in the Exchange parent directory and not in subdirectories.
Length of verification	A digit from 4 to 8 must be entered to define the length of CLI numbers for the search in LDAP in myPortal for Desktop and myPortal for Outlook. The highest number (8) can be configured for more exact search and improved system performance Default value: 4
Dial by name search local extension only	When this flag is checked the "dial by name" function is limited to the acting node (local function). When this flag is unchecked the old function is still available which considers all user in the network but playing the announcement only after selection of a local user.

Parameters	Description
Directory search cache expires in	Set the number of minutes or a range of minutes that the cache memory is used when searching for contacts. The range of minutes you can set is 1-60 minutes. When the value is "0" then this function is disabled.
Search by Phone Number	When this flag is checked you can search in directories by phone number.
TLS	
Using TLS for client connections	Due to network reasons it might be necessary to switch off the secure client server connection. Changing this setting requires a restart of the UC application. This should be done in very specific cases only!
Presence	
Hide sick status	When this flag is activated, the "sick" presence status is not available for use. Default value: Disabled
Username	
Disable name editing	When this flag is activated, users cannot change their configured first and last name. Default value: Disabled
Wallboard	
Disable Wallboard	When this flag is activated, the Wallboard is not available.
Display agent names in myAgent queue binding	When this flag is set, together with the extension number of an agent, a name also appears that the user can configure. A user will show "Hotdesk" when they are using an extension other than their own. Default value: Disabled.
Live Record	
Live Record	When this flag is activated, the recording of calls is possible. Default value: Enabled
Play prompt before recording	When this flag is activated, an announcement is played before a recording starts. Default value: Disabled
Play pip tone during recording	For OpenScape Business S, when this flag is activated, a warning tone is played during the recording. Default value: Enabled
Conference Live Recording availability	When this flag is activated, the recording of conferences is possible. Default value: Disabled
System Logging	

Parameters	Description
Log Trace Messages (Verbose)	When this flag is activated, trace messages are recorded in a log file on a daily basis. Default value: Disabled
Client Logs	
Client log path	Storage path for client log files (log files of the UC Suite)
Enable log upload	When this flag is activated, the client logs are stored on the hard disk of the UC Booster Card (OCAB), the UC Booster Server or the OpenScape Business S communication system. Default value: Enabled
Enable client logging	Activating this flag enables the recording of client logs. Default value: Enabled
Email Notifications	
Enable email notifications of system errors	When this flag is activated, E-mail notifications will be sent to the entered recipients to provide advance warnings about critical disk usage levels for the hard disk, for example, or about errors. Default value: Enabled
Enable myPortal invitation email	When this flag is activated, UC Suite users will be sent an invitation email to install or update the myPortal client. This email is normally sent to all UC Suite users with a valid email address in User Directory on a new installation, when an email address is added or changed for a UC Suite user in User Directory or after an OpenScape Business software update has occurred and a new version of the client is available. Default value: Enabled
Recipients	E-mail addresses of the individuals to whom e-mail notifications are to be sent.
Conditions	
Send Critical Messages	When this flag is activated, e-mail notifications are sent for critical messages (e.g., system errors) Default value: Enabled
Send Crash Notifications	When this flag is activated, e-mail notifications are sent for system crashes. Default value: Enabled
On error reporting, send the last … lines from the log file	Defines the number of lines of a log file to be sent by e-mail. Default value: 100
Maintenance	

Parameters	Description
Begin system maintenance at	Defines at what time the following data is deleted on a daily basis when the individual retention periods have expired: • Messages • Call information in the call journal (call history) • Calls recorded with myAgent (contact center) • Faxes and e-mails received and sent for the Contact Center • Log files Default value: 2.00 hours
Message	
Keep inbox messages for	Retention period in days for voice messages in the Inbox Default value: 60
Keep played / read messages for	Retention period in days for played/read voice messages Default value: 30
Keep saved messages for	Retention period in days for saved voice messages Default value: 365
Keep deleted messages for	Retention period in days for deleted voicemails Default value: 30
Fax	
Keep inbox faxes for	Retention period in days for faxes in the Inbox Default value: 30
Keep read faxes for	Retention period in days for read faxes Default value: 30
Keep deleted faxes for	Retention period in days for deleted faxes Default value: 30
Keep sent faxes for	Retention period in days for sent faxes Default value: 30
Calls Information Maintenance	
Keep call history for	Retention period in days for calls in the journal Default value: 30
Close conversation after	Retention period in days for open call conversations in the journal. Any unanswered calls from/to the same contact during this period will be added to the open calls tab, linked to the same conversation. After the end of this period, all calls in a conversation are marked as completed automatically and removed from open calls tab. Default value: 3 Maximum value: 30

Parameters	Description
Contact Center	Retention period in days for calls recorded with myAgent and for the faxes and e-mails received and sent for the Contact Center Default value: 30
Keep CC live record/ callback/email/fax calls for	Retention period in days for all communication data associated with calls, like callback messages, live recorded calls, fax calls and emails. Default value: 30
Log File Maintenance	
Keep log information for	Retention period in days for log files Default value: 10
Instant Message	
Keep instant messages for	Retention period in days for instant messages. Default value: 30
Reports	
Reset password	Resets myReports administrator password to the default password.
Reset all user password	
Reset all user password	Resets passwords for all users, allows for passwords up to 6 characters. **NOTICE:** In this case, the default password is set to 6 characters (123456).
VoiceMail	
VoiceMail Language	Default language of the voicemail box for the menu prompts and the internal system announcements
VoiceMail Message Play Order	Defines the sequence in which voicemail messages are played Default value: Newest First
VoiceMail Message Play Order: Newest First	The most recent voicemail message is presented first.
VoiceMail Message Play Order: Oldest First	The oldest voicemail message is presented first.
VoiceMail Message Recording time	Defines the maximum recording time for a voicemail message in seconds Default value: 900
VoiceMail Mode	Defines the functionality of the voicemail box Default value: Full
VoiceMail Mode: Full	Full functionality of the voicemail box
VoiceMail Mode: Short Menu	After the status-based or personal announcement is made, a connection to the operator is offered.

Parameters	Description
VoiceMail Mode : No VoiceMail Menu	After the greeting announcement is played, the caller is directly taken to the voice recording.
Allow callback from VM to known number only	When this flag is activated, any callers whose numbers are not stored in the UC client will be prevented from accessing the voicemail box. Default value: Enabled
Skip "please leave a message after the tone" prompt	When this flag is activated the "please leave a message after the tone" prompt will be skipped. Default value: Disabled
Contact Card Mapping	
Microsoft: Available(Green)	The presence UC status of this row is assigned to Available(Green) Outlook status.
Microsoft: Off Work(Yellow)	The presence UC status of this row is assigned to Off Work(Yellow) Outlook status.
Microsoft: Busy(Red)	The presence UC status of this row is assigned to Busy(Red) Outlook status.
Microsoft: Out of Service(Grey)	The presence UC status of this row is assigned to Out of Service(Grey) Outlook status.

28.4.4.14 OpenScape Business, UC Suite > Profiles

Parameter Description of Tabs:

- **Add / Edit**

Parameters	Description
Profiles	User profiles store the settings of the UC Suite users. One or more users (members) can be assigned to a user profile. All members of this profile have the same settings (at first). Multiple profiles can be created to define different settings for different user groups.
Name	Name of the profile (free input)
Personal Details	
My Personal Details	Selected personal data for the assigned users. The lock symbol determines whether users can change these settings themselves.
My Preferences	
Appearance	Skin and language of the UC client of the associated user. The lock symbol determines whether users can change these settings themselves.
Notification	Notifications for the assigned users. The lock symbol determines whether users can change these settings themselves.
Outlook Connectivity	Calendar integration for the assigned users. The lock symbol determines whether users can change these settings themselves.

Parameters	Description
Hot Keys	Activation and set up of key combinations for access to various commonly used functions through the keyboard. The lock symbol determines whether users can change these settings themselves.
Miscellaneous	Automatic return to the presence status "Office"; transfer method and retention period of the call journal for the assigned users. The lock symbol determines whether users can change these settings themselves.
Call Rules	
Forwarding destinations	Forwarding destinations for incoming calls for the assigned users, depending on the presence status. The lock symbol determines whether users can change these settings themselves.
Communications	
Voicemail settings	Recording of voice messages for the assigned users, depending on the presence status. The lock symbol determines whether users can change these settings themselves.
VM Notification	Notification of new voice messages for the assigned users. The lock symbol determines whether users can change these settings themselves.
Fax Notification	Notification of new fax messages for the assigned users. The lock symbol determines whether users can change these settings themselves.
Missed Call Notifications	Notification Service for Missed Calls.
VoiceMail Profiles	
VoiceMail Profiles	Personal AutoAttendant for the assigned users. The respective users must record an announcement for the selection. The lock symbol determines whether users can change these settings themselves.
Sensitivity	
Security and Access	Allow listening to voicemail with myAttendant and checking the voicemail box from the own phone without a password. The lock symbol determines whether users can change these settings themselves.
Presence Visibility	Internal subscribers who are allowed to see the presence status. The lock symbol determines whether users can change these settings themselves.
VoiceMail Presence	Internal or external callers who are to be informed about the presence status through automated announcements of the voicemail box. The lock symbol determines whether users can change these settings themselves.
Favorites	
Favorites	Favorite groups with a list of contacts that can be assigned to the user.

Parameter Description of Tabs:

- **Assign Users**

Parameters	Description
Assigned Users	Users to whom the profile applies

Parameters	Description
Available Users	Users to whom the profile can be applied

Parameter Description of Tabs:

- **Remove**

Parameters	Description
Name	Name of the profile (free input)
Users	Users to whom the profile applies

28.4.4.15 OpenScape Business, UC Suite > Fax Headlines

Parameter Description of Tabs:

- **Edit**
- **Add**
- **Remove**

Parameters	Description
Template Name / Name	Name of the header (must be unique).
Text	Placeholders for the date/time, company name, user name, company phone number, page number and number of pages can be inserted.

28.4.5 Web Services

The functions for configuring of the web interfaces such as Web Collaboration, for example, are grouped under **Web Services**.

28.4.5.1 Web Services > Web Collaboration

For the integration of web collaboration via a public server (web collaboration server as a service on the Internet) or via a custom server (web collaboration server in the customer network or with a partner).

Parameter Description of Tabs:

- **Web Collaboration Server**

Parameters	Description
Server Type	Selection of the web collaboration server.
Server Type: **Public Server**	The web collaboration server is a public server and is located on the Internet. A secure https connection is used for this. In addition, a license number and a password are required. By default, TCP port 5100 is used for this purpose.
Server Type: **Public Server (Demo Mode/Evaluation Mode)**	The web collaboration can be tested for 5 minutes. No input of an IP address, license number and password are required for this.

Parameters	Description
Server Type: **Custom Server**	The web collaboration server is a custom server and is located in the customer network or with a partner. Either a secure https connection or an unsecured http connection can be used for this. When connecting via https, a license number and a password are additionally required. By default, TCP port 5004 is used for this purpose.
Server Type: **No Web Collaboration Server**	No web collaboration server is being used. The option to start a web collaboration session is disabled in the UC clients.

URL / IP address	Enter the URL or IP address of the appropriate web collaboration server. Public server via https and custom server via http or https.
	Example:
	`http://<web collaboration server IP address>:5004/OscInterface`
	`https://<web collaboration server IP address>:5100/XMLRPSecure`

License number	License number for the secure connection to the web collaboration server.
Password	Password for the secure connection to the web collaboration server.

28.4.6 Open Directory Service

The functions for configuring the Open Directory Service are grouped under **Open Directory Service**.

28.4.6.1 Open Directory Service > Basic Settings

Parameters	Description
Enable/Disable Open Directory Service	Default value: disabled
LDAP server login credentials	Login data of the external database server. Open Directory Service must be authorized to access the external database; if necessary, a separate user account must be added on the server for this purpose.

28.4.6.2 Open Directory Service > Data Sources > OpenScape Business Users

Parameter Description of Tabs:

- **Overview of the configured data sources**

Parameters	Description
OpenScape Business Users	Internal directory of UC Suite. The directory is permanently assigned to the Open Directory Service and cannot be deleted or changed.

Parameters	Description
UC Suite External Directory	External data source for UC Suite systems. The directory is permanently assigned to the Open Directory Service and cannot be deleted or changed.
Global Directory	Global directory data source for non-UC Suite systems. The directory is permanently assigned to the Open Directory Service and cannot be deleted or changed.
Speed Dials	Central speed-dial numbers. The directory is permanently assigned to the Open Directory Service and cannot be deleted or changed.
Add/Edit/Delete	External data sources for contact information from databases with read access via ODBC.

Parameter Description of Tabs::

- **Edit data source**

Parameters	Description
New data source	The parameters of the added data sources can be changed here.

28.4.6.3 Open Directory Service > Data sources > LXV3

Parameters	Description
Speed Dials	Central speed-dial numbers. The directory is permanently assigned to the Open Directory Service and cannot be deleted or changed.

28.4.6.4 Open Directory Service > Data sources > LXV3

Parameters	Description
Overview of the configured data sources	An LDAP data output mapping determines which of the fields in the data schema of the Open Directory Service are to be output via LDAP, e.g., for specific LDAP clients or for different groups of subscribers who do not want to see all the details, but only a defined subset. The LDAP data output mapping "web" is available by default and cannot be deleted or changed. All fields of the data schema in the Open Directory Service are permanently assigned to the LDAP output in it. You can also configure other LDAP data output mappings.
Add	Add more data output mappings. LDAP clients can access a specific LDAP data output mapping via the dc parameter in the LDAP login, for example: dc=web.

28.4.6.5 Open Directory Service > Maintenance

Parameter Description of Tabs:

- **Maintenance**

Parameters	Description
Check/Restart Open Directory Service	Status indicator of the Open Directory Service (grey = disabled, red = incorrect configuration or data source not available, green = enabled)
Restart	Restart the Open Directory Service

28.4.7 Application Launcher

The functions for configuring Application Launcher are grouped under **Application Launcher**.

28.4.7.1 Application Launcher

Parameters	Description
Upload Configuration File	Profile with configuration data for Application Launcher to enable the easy and fast configuration of Application Launcher on all client PCs. As soon as Application Launcher has been fully configured for an initial user, as an administrator, you can make that profile with the Application Launcher configuration data available in the communication system. All other users can then perform the configuration of Application Launcher by importing this profile.
Profile	Allowed file type .xml

28.5 Middleware

The functions for configuring the middle-ware are grouped under **Middleware**.

28.5.1 Announcement Player

Parameter Description of Tabs:

- **Announcement player settings**
- **Announcement player statistics**

Parameters	Description
Activation	
Service will be started automatically	Activation or deactivation of the playback device for announcements.
Announcement player statistics	The status of the announcement device is displayed here. The data is automatically updated every 5 minutes. However, the page can also be refreshed manually.

28.5.2 Csta Message Dispatcher (CMD)

Parameter Description of Tabs:

- **CSTA Message Dispatcher (CMD) settings**
- **CSTA Message Dispatcher (CMD) Statistics**

Parameters	Description
Activation	
Service will be started automatically	Activation or deactivation of the CSTA Message Dispatcher (CMD). The CMD sets up the connection between the OpenScape Business TAPI 120 clients and the communication system and is required for the functionality.
Auto Registration	
Client auto registration enabled	Enable or disable the automatic registration of the clients. Automatic registration means that new entries are possible in the list of CTI firewall, and the CTI firewall is thus configured automatically. When all authorized clients have registered, the check mark can be removed, and new entries in the CTI firewall can be prevented. A PC can be authorized to control a specific extension. The TAPI/CTI licenses must be additionally assigned.
CTI firewall	
Delete	Entries with a check mark in the Delete column are removed from the list of authorized clients on clicking the **Apply** button. An login will then be rejected, unless the automatic registration is enabled.
Application ID	Name of the PC from which an extension can be controlled. By using the PC name, DHCP can also be used for the OpenScape Business TAPI 120 PCs.
Call number	Internal call number of the extension to be controlled.
CSTA Message Dispatcher (CMD) Statistics	The status of the CMD is shown here. During the current operation, it is possible to verify for which of the OpenScape Business TAPI 120 connected to the CMD licenses may need to be assigned. The data is automatically updated every 5 minutes. However, the page can also be refreshed manually.

28.5.3 Csta Service Provider (CSP)

Parameter Description of Tabs:

- **Csta Service Provider (CSP) settings**
- **CSTA Service Provider (CSP) Statistics**

Parameters	Description
Activation	
Service will be started automatically	Activation or deactivation of the CSTA Service Provider (CSP). The CSP is required for the UC Suite, the DSS server (Presence Manager, only in networking), the OpenScape Business TAPI 170 and external CSTA applications.

Parameters	Description
CSTA Access	
CSTA user ID / **CSTA user password**	OpenScape Business TAPI 170 and external CSTA applications can only log in at the CSP with the user account configured here. If no CSTA user is configured, it is not possible to use OpenScape Business TAPI 170 or external CSTA applications at the CSP.
CSTA Service Provider (CSP) Statistics	The status of the CSP is shown here. You can see how many and which applications are connected with the CSP. Unknown applications are represented with 'Default'. The connection status to the individual nodes of the network or the local node can be displayed. The data is automatically updated every 5 minutes. However, the page can also be refreshed manually.

28.5.4 DSS Server

Parameter Description of Tabs:

- **DSS Server settings**
- **DSS Server Statistics**

Parameters	Description
Activation	
Service will be started automatically	Enable or disable the DSS server.
DSS Server Statistics	The status of the DSS server is displayed here. The data is automatically updated every 5 minutes. However, the page can also be refreshed manually.

28.5.5 Media Extension Bridge (MEB)

Parameter Description of Tabs:

- **Media Extension Bridge (MEB) settings**
- **Media Extension Bridge (MEB) Statistics**

Parameters	Description
Activation	
Service will be started automatically	Enable or disable the Media Extension Bridge.
Media Extension Bridge (MEB) Statistics	The status of the MEB is displayed here. The data is automatically updated every 5 minutes. However, the page can also be refreshed manually.

29 Appendix

This appendix contains reference information such as the supported languages, standards, configuration limits and capacities, Euro-ISDN features, codes for enabling and disabling features, feature codes using DTMF and the IP protocols and port numbers used.

29.1 Supported Standards

This section contains information on the supported standards.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q Virtual LANs
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3X Full Duplex Operation

IP Routing

- 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 A 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 PHB (Per-Hop Behavior)

Services

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Codecs

- G.711
- G.729

VoIP over 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

Other

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

29.2 Euro-ISDN Features

The Euro-ISDN features can be used at every Euro-ISDN port if the available hardware (phone or ISDN card, for instance) is appropriately configured. The features are either available permanently in the Central Office or activated/ deactivated with codes.

The availability of features depends on the network provider. Some of the named features are subject to charges.

Topic	Explanation
Multiple Subscriber Number (MSN)	Every point-to-multipoint connection can be assigned several phone numbers. The user can assign these phone numbers to the individual terminals directly at the terminals.
Calling Line Identification Presentation (CLIP)	The actual phone number is transmitted to the called station and appears, for example, on the phone's display or in the caller list if the call is not answered. Incorrect phone numbers cannot be transmitted. Direct inward dialing from TC systems cannot be checked, however. Phone number transmission can be suppressed on a case-by-case basis or for all calls.
Calling Line Identification Restriction (CLIR)	Phone number transmission can also be deactivated either permanently or on a case-by-case basis. If deactivated, phone numbers are only displayed at specially defined B stations (emergency help lines, police, fire department).
Malicious Call Identification (MCID)	The called party can have an anonymous caller traced by the attendant console, even if phone number transmission is deactivated. A charge is applied for this feature.
Terminal Portability (TP)	This feature lets you move the ISDN phone you are using and plug it into a different ISDN jack without interrupting an ongoing call. You must park the ongoing call before you move the ISDN phone.
Subaddressing (SUB)	This function is subject to an additional charge and can be used in addition to the normal phone number. Subaddressing lets you operate a dialable phone (for example, a program on the PC) depending on the caller.

Topic	Explanation
User to User Signaling (UUS)	Information can be exchanged over the D channel during connection setup and clear-down. Transmission is possible in both directions.
Closed User Group (CUG)	If you activate this feature, no calls are possible outside the user group (apart from the emergency numbers 110 and 112). External callers can also be blocked.
Call Forwarding Busy (CFB)	This call forwarding variant routes calls on busy to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call Forwarding Unconditional (CFU)	This call forwarding variant routes calls immediately to an arbitrary available phone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call Forwarding No Reply (CFNR)	This call forwarding variant routes calls after 20 seconds (if the destination cannot be reached) to an arbitrary available telephone. Call forwarding is performed in the attendant console. This leaves both B channels free.
Call waiting (CW)	A second caller is signaled during an ongoing connection. The caller meanwhile hears the ringback tone. The camp-on connection can be accepted, declined or simply ignored.
Toggle (Hold = Call Hold)	The Consultation feature lets you set up a second connection while another connection is already ongoing. Switching back and forth between two connections is known as toggling. The party on hold cannot overhear the other active call.
Three Party Service (3-PTY)	Two existing connections can be joined together. A three-party conference can be conducted by three subscribers.
Completion of Calls to Busy Subscriber (CCBS; automatic callback on busy)	You can activate this feature if a station called is busy. You hear a signal as soon as this station's port is free. The connection is cleared down by replacing the handset.
Advice of Charge (End) (AOCE)	You can program the application to display call charges at the end of a call. This does not take account of any discounts or tariffs.
Advice of Charge (During) (AOCD)	You can program the application to display call charges during a call. This does not take account of any discounts or tariffs.

29.3 Used Ports

The OpenScape Business system components use different ports, which may need to be opened in the firewall as required. For the ports of the web-based clients (e.g., myPortal to go), port forwarding must be configured in the router.

An actual and complete list of all used ports of OpenScape Business is available in the "Interface Management Database" (IFMD) which can be accessed via the Partner Portal of Unify (https://unify.com/en/partners/partner-portal.

NOTICE: The ports identified with "O" in the list below are optional, i.e., are not permanently open in the firewall.

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
System components							
Admin Portal (https)	X		443	X	X	X	X
CAR Alive checks	X		12062	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CLS	X		7780, 7790 (up to V3R3) 7780, 7791 (V3R3.1 and higher)	O		O	
Communication Client Installer	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	O		O	
FTP Passive	X		40000-40040	O		O	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	X	X

Description	TCP	UDP	Port number	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP server	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
OpenScape Business status server	X		8808	X		X	X
OpenScape Business user portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (embedded)		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 for Clients	X		8803	X	X	X	X
Web-based clients							
Web-based clients (http)	X		8801	X	X	X	X
Web-based clients (https)	X		8802	X	X	X	X

NOTICE: For security reasons, we recommend that only https be used for the web-based clients and that port forwarding be set up from external TCP/443 to internal TCP/8802.

CLS certificate

Starting with V3R3.1, a new CLS certificate with an updated Common Name (CN) is provided via a newly introduced port. This offers an improved and stronger digest algorithm as well as updated legal entities. Systems licensed online via CLS Connect mode, require the following two prerequisites:

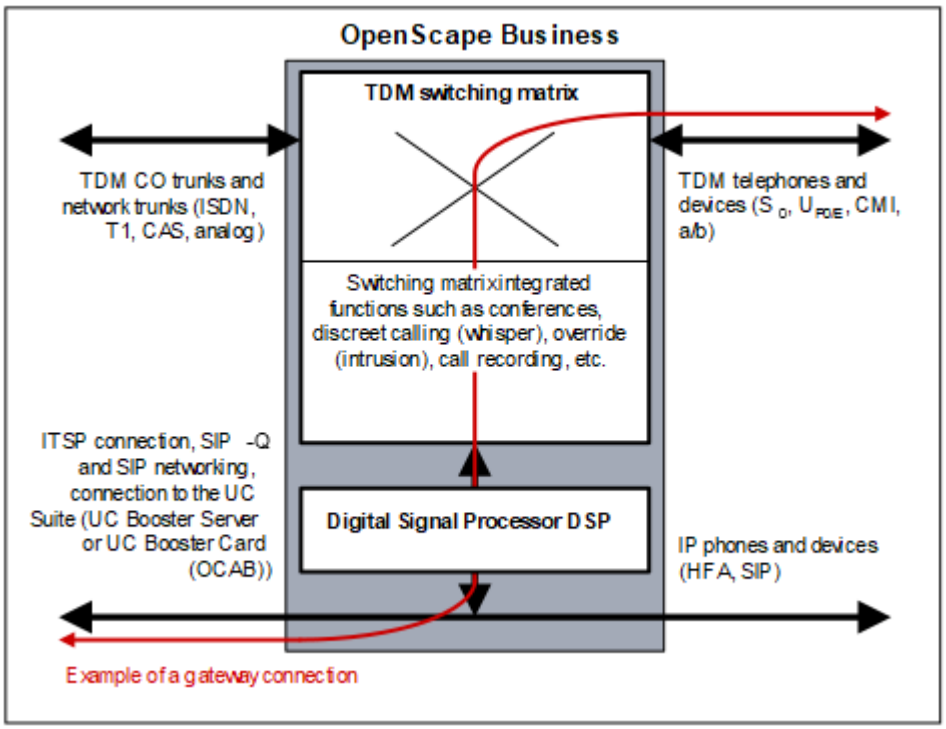
- The IP address 188.64.16.4 is enabled for outgoing traffic in the firewall.
- Ports 7780 and 7791 are enabled for outgoing traffic in the firewall.

The previously used port 7790 can be removed from the firewall configuration after the upgrade to V3R3.1 to increase security.

29.4 Project Planning of DSP Channels for the OpenScape Business X3/ X5/X8 Communication Systems

Connections between IP and TDM phones/trunks are "gateway connections"; each gateway connection requires one DSP (Digital Signal Processor) channel. In addition, DSP channels are required on activating the Signaling And Payload Encryption (SPE) feature.

No DSP channels are required for pure TDM connections and IP-only connections.



The mainboards of the OpenScape Business X3/X5/X8 communication systems provide a maximum eight DSP channels.

If the DSP channels of a mainboard are not sufficient, additional channels can be provided by plugging in a Voice Channel Booster Card (OCCB1 or OCCB3 subboard):

- OCCB1 provides up to 40 additional DSP channels.
- OCCB3 provides a maximum of 120 additional DSP channels.

The number of DSP channels available for gateway connections is reduced by the use of the G.729 codec and when using Signaling and Payload Encryption (SPE).

Ultimately, the number of simultaneous gateway connections (simultaneous voice connections with IP-TDM transition) determines whether and which OCCB subboard should be used.

In the case of UC-Suite conferencing and IP Phones, an OpenScape Business X3/X5/X8 communications system can include up to eight DSP channels. By default three DSP channels are alocated for the 3 default codecs of Music on Hold. This number can be reduced if you use less codecs for Music on Hold. In addition, two DSP channels are reserved for the configuration of the Signaling and Payload Encryption (SPE). The rest of the DSP channels can be alocated for IP phones (one DSP channel per IP phone). When the available DSP channels are exhausted, the number of DSP channels can be increased with the use of the corresponding OCCB cards (OCCB1 or OCCB3 as stated previously).

INFO: For more details on the maximum DSP channels available on the mainboard and the OCCB subboards, see System-Specific Capacity Limits.

The undersizing of DSP channels can result in DSP bottlenecks that typically manifest themselves through busy states when setting up connections (busy tone during call setup, display showing `Not currently possible`).

When a DSP bottleneck occurs, an entry is made in the event log file of the communication system.

The following measures should be taken if DSP bottlenecks occur frequently:

If	Then
The DSP channels on the mainboard are being used.	Insert the OCCB1 or OCCB3 subboard into the mainboard.
The DSP channels on the mainboard and the OCCB1 subboard are being used.	Insert the OCCB3 subboard into the mainboard.
The DSP channels on the mainboard and the OCCB3 subboard are being used.	Check whether the communication system can be operated only with the G.711 codec. This increases the number of DSP channels to the maximum. ***INFO:*** The **Use G.711 only** option can be activated by an administrator with the **Expert** profile in **Expert Mode** (**Telephony** > **Voice Gateway** > **Codec Parameters**).

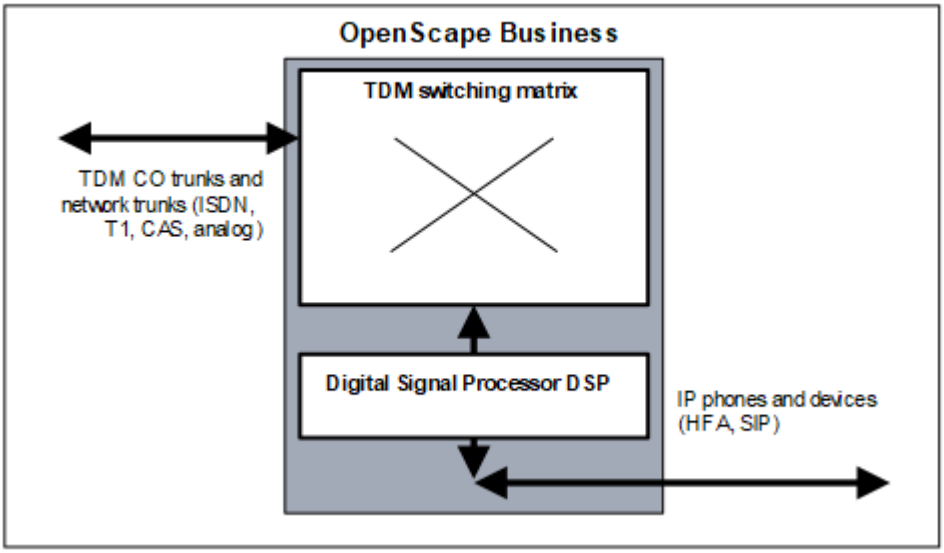
The following table provides orientation values for which OCCB subboard, if any, should be used.

Sum of the TDM channels: CO trunks and network trunks (ISDN, T1, CAS, analog)	**Sum of IP channels:** ITSP connection, SIP-Q and SIP networking, connection to the UC Suite (UC Booster Server or UC Booster Card (OCAB))	**Sum of TDM telephones and TDM devices (S_0, $U_{P0/E}$, CMI, a/b)**	**Sum of IP phones and devices (HFA, SIP)**	**Which OCCB subboard?**	**Notes**
Any number	Announcements (up to 16) 0	Any number	0	No OCCB subboard	Smart VM and system conferences are processed through the switching matrix.
			up to 8	No OCCB subboard	Independent of the TDM channels. Smart VM and system conferences in combination with IP phones and IP devices require DSP resources.
			9 to 100	OCCB1	Independent of the TDM channels. Smart VM and system conferences in combination with IP phones and IP devices require DSP resources, up to 40 simultaneously.
			> 100	OCCB3	Independent of the TDM channels. Smart VM and system conferences in combination with IP phones and IP devices require DSP resources, up to 120 simultaneously.
	> 0	up to 8		No OCCB subboard	
	> 0	9 to 100		OCCB1	Up to 40 simultaneously
	> 0	> 100		OCCB3	Up to 120 simultaneously

Sum of the TDM channels: CO trunks and network trunks (ISDN, T1, CAS, analog)	Sum of IP channels: ITSP connection, SIP-Q and SIP networking, connection to the UC Suite (UC Booster Server or UC Booster Card (OCAB))	Sum of TDM telephones and TDM devices (S_0, $U_{P0/E}$, CMI, a/b)	Sum of IP phones and devices (HFA, SIP)	Which OCCB subboard?	Notes
> 0	up to 8			No OCCB subboard	The combination is essentially relevant for SIP-Q and UC Suite.
> 0	up to 9			OCCB1	The combination is essentially relevant for SIP-Q and UC Suite.
> 0	> 40			OCCB3	The combination is essentially relevant for SIP-Q and UC Suite.

The following examples provide orientation values for which OCCB subboard, if any, should be used.

Example 1: OpenScape Business with TDM Trunks and IP Phones and Devices

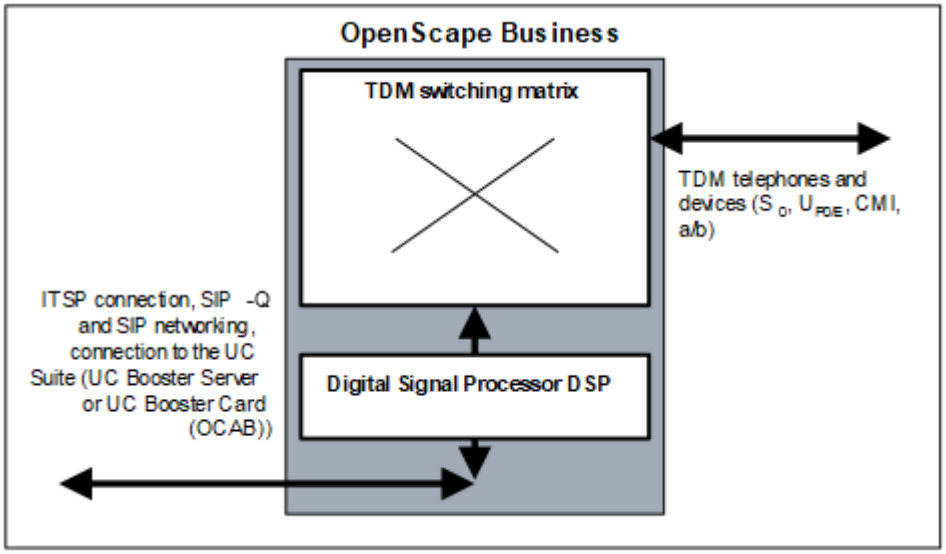


If	Then
OpenScape Business with: • 1 x TDM-CO (ISDN) • 20 x IP telephones (HFA, SIP)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.

If	Then
OpenScape Business with: • 1 x TDM-CO (ISDN) • 100 x IP telephones (HFA, SIP)	Subboard OCCB1 is required. Alternatively, the OCCB3 subboard can be used.
OpenScape Business with: • 2 x TDM-CO (ISDN) • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.
OpenScape Business with: • 4 x TDM-CO (ISDN) • 500 x IP telephones (HFA, SIP)	Subboard OCCB3 is required. ***NOTE:*** In order to achieve the maximum number of DSP channels, only the G.711 codec may be used in this system configuration.

If the communication system is to be equipped with TDM phones and devices as well (S_0, $U_{P0/E}$, CMI, a/b), additional DSP channels for this must be taken into account.

Example 2: OpenScape Business with ITSP Connections and TDM Phones and Devices

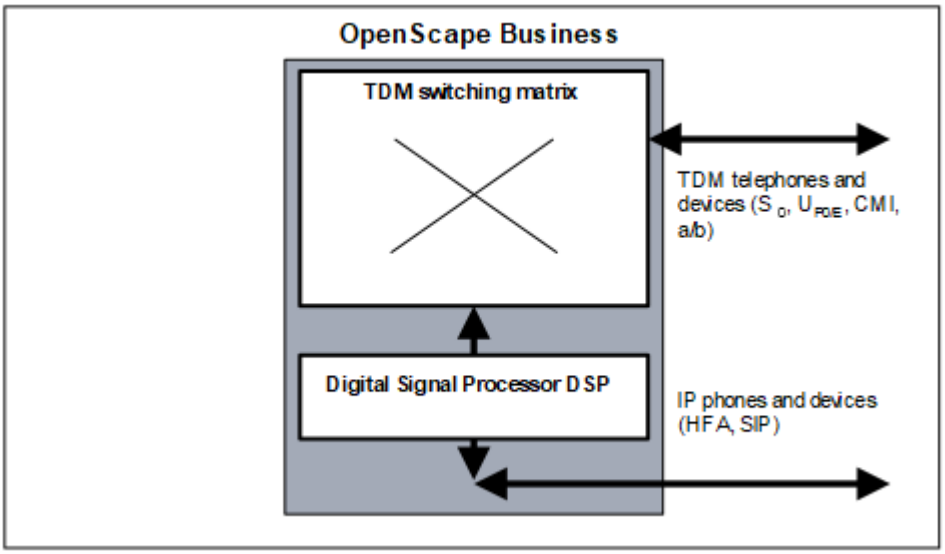


If	Then
OpenScape Business with: • 6 x ITSP connections (6 B channels) • 20 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.

If	Then
OpenScape Business with: • 30 x ITSP connections (30 B channels) • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB1 is required. Alternatively, the OCCB3 subboard can be used.

If the communication system is to be equipped with IP phones and devices as well (HFA, SIP), additional DSP channels for this must be taken into account.

Example 3: OpenScape Business with TDM Phones and Devices and IP Phones and Devices



If	Then
OpenScape Business with: • 6 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b) • 6 x IP telephones (HFA, SIP)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.
OpenScape Business with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b) • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.

If the communication system is to be equipped with TDM trunks or IP trunks as well, additional DSP channels for this must be taken into account.

Example 4: SIP-Q Networking with OpenScape Business

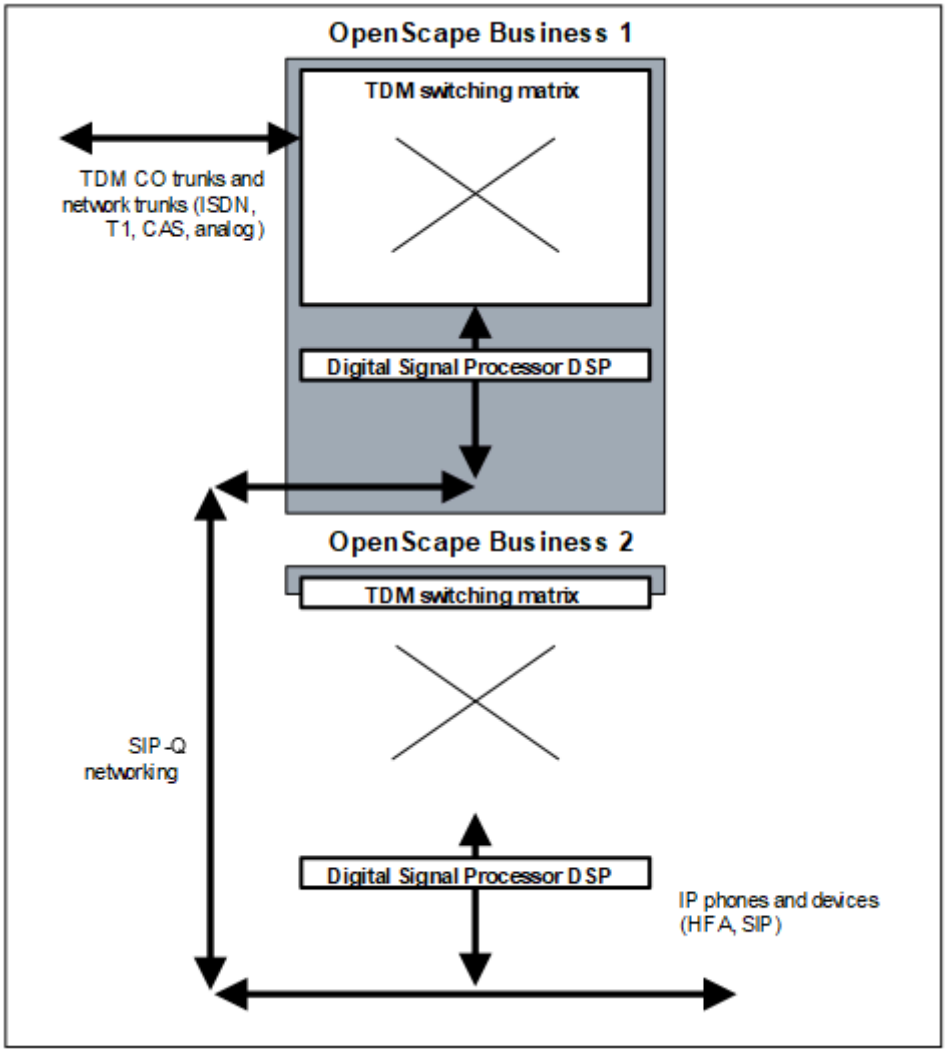
NOTICE: This example presents requirements of a networked second OpenScape Business system. Connections in the first system are not depicted here for the sake of simplicity. However,

the requirements of the first system, as stated in examples 1, 2, and 3 must be taken into consideration also.

The OpenScape Business 1 communication system acts as a gateway for TDM Central Office.

IP phones (HFA, SIP) are connected only to the OpenScape Business 2 communication system.

Depending on the number of IP phones at the OpenScape Business 2 communication system, the DSP channels for the OpenScape Business 1 communication system must be planned. DSP channels are required exclusively in the TDM gateway.



If	Then
OpenScape Business 1 with: • 1 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB1 is required in OpenScape Business 1. Alternatively, the OCCB3 subboard can be used. No OCCB subboard is required in OpenScape Business 2.

If	Then
OpenScape Business 1 with: • 2 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required in OpenScape Business 1. No OCCB subboard is required in OpenScape Business 2.
OpenScape Business 1 with: • 4 x TDM-CO (ISDN) OpenScape Business 2 with: • 500 x IP telephones (HFA, SIP)	Subboard OCCB3 is required in OpenScape Business 1. ***NOTE:*** In order to achieve the maximum number of DSP channels, only the G.711 codec may be used in this system configuration. No OCCB subboard is required in OpenScape Business 2.

If the OpenScape Business 2 communication system is to be equipped with TDM trunks or TDM phones and devices (S_0, $U_{P0/E}$, CMI, a/b) as well, additional DSP channels must be taken into account for this.

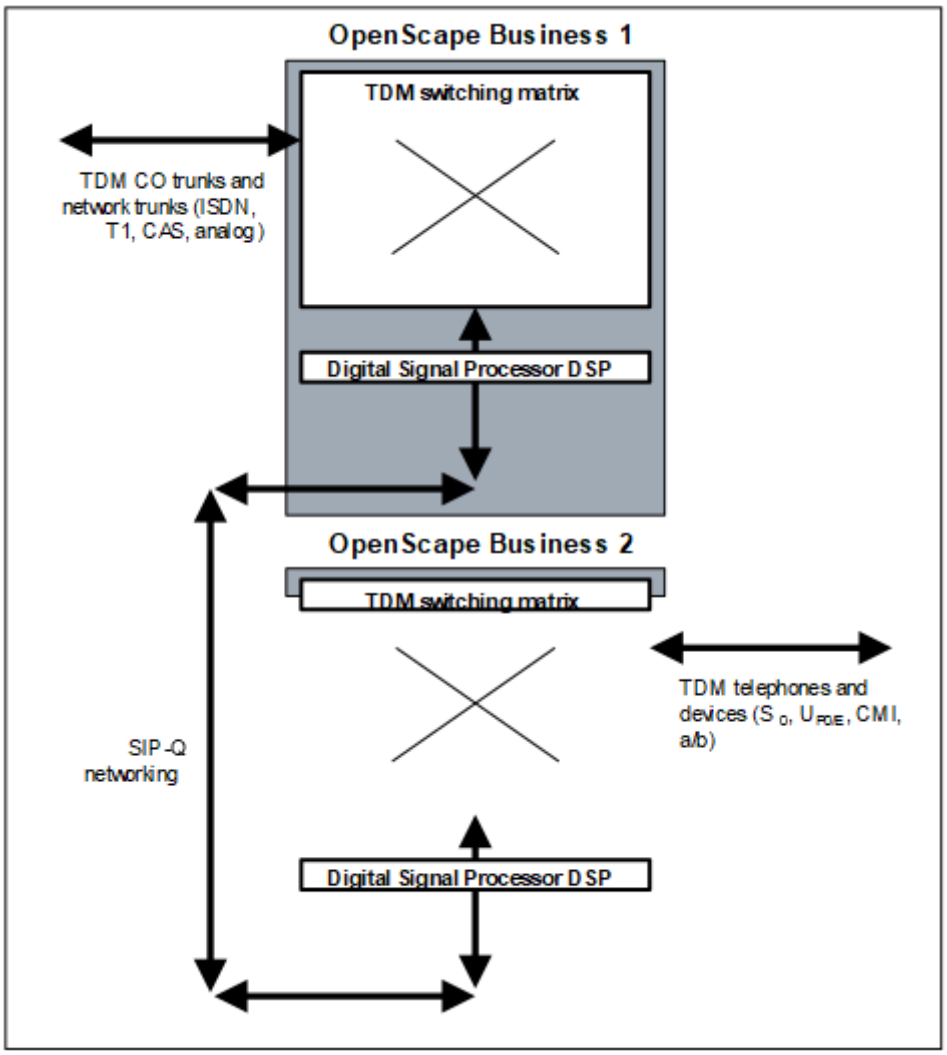
Example 5: SIP-Q Networking with OpenScape Business

NOTICE: This example presents requirements of a networked second OpenScape Business system. Connections in the first system are not depicted here for the sake of simplicity. However, the requirements of the first system, as stated in examples 1, 2, and 3 must be taken into consideration also.

The OpenScape Business 1 communication system acts as a gateway for TDM Central Office.

TDM phones (S_0, $U_{P0/E}$, CMI, a / b) are connected only at the OpenScape Business 2 communication system.

Since gateway connections are required in both communication systems (OpenScape Business 1: TDM CO <-> SIP-Q Networking, OpenScape Business 2: SIP-Q Networking <-> TDM phone), DSP channels are needed in both systems.



If	Then
OpenScape Business 1 with: • 1 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB1 is required in OpenScape Business 1 and OpenScape Business 2. Alternatively, the OCCB3 subboard can be used in both cases.
OpenScape Business 1 with: • 2 x TDM-CO (ISDN) OpenScape Business 2 with: • 100 x TDM telephones (S_0, $U_{P0/E}$, CMI, a/b)	Subboard OCCB3 is required in OpenScape Business 1 and OpenScape Business 2.

If the OpenScape Business 1 communication system is to be equipped with TDM phones and devices (S_0, $U_{P0/E}$, CMI, a/b) as well, additional DSP channels must be taken into account for this.

Example 6: OpenScape Business with IP Phones and Devices

NOTICE: This example presents requirements of a networked second OpenScape Business system. Connections in the first system are not depicted here for the sake of simplicity. However, the requirements of the first system, as stated in examples 1, 2, and 3 must be taken into consideration also.

If	Then
OpenScape Business X3/X5/ X8 with: • 7 x IP telephones (HFA, SIP)	The DSP channels on the mainboard are sufficient. No OCCB subboard is required.
OpenScape Business: • 30 x IP telephones (HFA, SIP)	Subboard OCCB1 is required.Alternatively, the OCCB3 subboard can be used.
OpenScape Business with: • 100 x IP telephones (HFA, SIP)	Subboard OCCB3 is required.

30 Glossary

The glossary provides short explanations of the terms used (for instance, protocols and standards).

30.1 Glossary

10BaseT, 100BaseT, 1000BaseT

This refers to a specification (IEEE. 802.3i)) for networks with 10 Mbps base band transmission over a symmetrical 100-Ohm four-wire cable. 100BaseT, on the other hand, is used for bandwidths of up to 100 Mbps and 1000BaseT for bandwidths of up to 1000 Mbps.

AES (Advanced Encryption Standard)

AES is a symmetric encryption system that was ratified by the National Institute of Standards and Technology as the successor to the earlier DES and 3DES Standards. It is used for VPN, for example.

ADSL with dynamic IP address

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. A dynamic IP address is sufficient if the web and mail services are provided by the Internet Service Provider.

ADSL with fixed IP address

ADSL stands for Asymmetric Digital Subscriber Line and means that the bandwidths from the Internet (download, downstream) and to the Internet (upload, upstream) are different. The classic Internet telephony connection is ADSL. ADSL with a fixed IP address is required if you want to run your own web and mail server on your site.

AF-EF (Expedited Forwarding - Assured Forwarding)

The codepoints AF and EF define the various priorities of IP packets for QOS (Quality of Service).

AF: guarantees minimum bandwidth for the data

EF: guarantees constant bandwidth for this data.

ARP (Address Resolution Protocol)

The Address Resolution Protocol (ARP) is a network protocol that facilitates the assignment of network addresses to hardware addresses. Although it is not limited to Ethernet and IP protocols, it is almost exclusively used in conjunction with IP addressing in Ethernet networks.

Authentication

Authentication is the verification of a person's or PC's identity. The check can be performed with a simple user name, for example, as well as with a fingerprint.

Authorization

Authorization is a mechanism for granting rights, e.g., access rights in a data network.

B channel

A B channel is the transmission path for the payload (voice, data) of an ISDN connection.

Busy Lamp Field (BLF)

myPortal provides a so-called Busy Lamp Field (BLF) to display the call status of the specified subscribers.

Broadcast

A broadcast is a message sent to everyone in a PC network. The message (i.e., a data packet) is transmitted from one point to all subscribers in the network. A broadcast is mainly used in a data network if the address of the message recipient is unknown.

CA (Certification Authority)

The CA is an organization that issues certificates with digital signatures. Digital signatures are required for a VPN (Virtual Private Network), for example.

CAPI Interface (Common Application Programming Interface)

CAPI is an ISDN-compliant standardized software interface. CAPI enables the development of ISDN software without requiring any knowledge about the manufacturer-specific ISDN hardware being used.

Centrex

Centrex (Central Office Exchange) provides the functions of a telephone system via a PSTN or ITSP. This is also known as virtual telephone system, hosted PBX (Private Branch Exchange) or NetPBX.

CHAP (Challenge Handshake Authentication Protocol)

CHAP is an authentication protocol used within the framework of the Point-to-Point protocol.

COS (Classes Of Service)

QoS is a procedure that ensures the transmission quality for data in IP networks.

CLIP (Calling Line Identification Presentation)

With station number transmission, the caller's phone number is displayed on the called party's station. The called party can therefore identify the caller before picking up the call.

CLIR (Calling Line Identification Restriction)

The caller suppresses the display of his or her call number on the called station. As a result, the called party cannot identify the caller before picking up the call.

COLP (Connected Line Identification Presentation)

With Connected Line Identification Presentation, the called party's number is displayed for the caller if the connection is successful.

COLR (Connected Line Identification Restriction)

With Connected Line Identification Restriction, the called party's number is not displayed for the caller, even if the caller activated COLP.

Comfort User

Comfort User is the standard user of the communication system.

Comfort Plus User

The Comfort Plus User is the Advanced User of the communication system. In contrast to the Comfort User, the Comfort Plus User can use more features (such as Fax, Mobility and Conferencing).

CorNet

CorNet is a proprietary protocol for networking the HiPath and OpenScape communications systems. In contrast to the generally supported QSIG, all manufacturer-specific features of the HiPath and OpenScape communication systems are integrated in CorNet.

CorNet-IP

CorNet-IP is a protocol variant of CorNet that enables the cross-networking of systems or the connection of system telephones (such as optiPoint) over IP.

CorNet-NQ

A proprietary QSIG-based signaling protocol for interconnecting communication systems to one or more QSIG PBX systems.

CSTA (Computer Supported Telecommunications Applications)

CSTA is a protocol interface for applications that support the European Computer Manufacturers' Association (ECMA) standard. Telecommunication tasks are controlled and monitored using SIP via CSTA.

CSV (Character Separated Values)

A CSV file is a text file for saving or exchanging simply structured data. CSV stands for Character Separated Values, Comma Separated Values or Colon Separated Values, since the individual values are delimited by a special separator character such as a comma or semicolon. CSV files must be available in ANSI/ASCII format.

CRL (Certificate Revocation List)

A CRL or Certificate Revocation List is a list or all revoked certificates. CRLs always have to be generated by the certification authority where the certificates originate.

Delay

A delay has two meanings in telecommunications:

- The delay by which an event is postponed.

- The time between the occurrence of an event and the appearance of a expected follow-on event.

Dedicated (Permanently Assigned) Gateway

If a dedicated gateway is entered in the LCR for a route, then routing via this gateway is enforced. All contradictory rules are then invalid for the routing.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a procedure by which a PC is assigned a certain IP configuration (IP address, subnet mask, etc.) at startup.

DS (DiffServ, Differentiated Services)

DS is a procedure for managing packets in data networks. The routing method for a specific data packet is specified as is a particular service level in regard to bandwidth, queuing theory, and packet discard decisions.

Diffie-Hellman algorithm

The Diffie-Hellman algorithm is used for the exchange of keys in a VPN. The data produced by this algorithm is configured with a specific set of mathematical parameters. The key exchange only works properly if both subscribers use identical values for these parameters.

DLI (Deployment License Service Integrated)

DLI enables the unattended installation and upgrading of IP system telephones.

DMZ (Demilitarized Zone)

A demilitarized zone (DMZ) refers to a PC network that offers a number of security features for accessing connected network nodes (PCs, routers, etc.).

DNS (Domain Name Service)

Name resolution on the Internet and in the LAN. DNS translates the names of PCs or web pages into the relevant IP addresses.

DSL (Digital Subscriber Line)

DSL is a technological solution for providing high-bandwidth Internet access. Internet telephone bridges the gap between the provider's attendant and the customer's telephone jack.

DSS (Direct Station Selection)

The function keys on a telephone or add-on device can be programmed as Direct Station Select (DSS) keys. These are programmed with the phone number of an internal subscriber or a group for this. Pressing a DSS key initiates an immediate call to the programmed destination.

DTMF (Dual Tone Multifrequency)

See DTMF.

EIM (Enterprise Instant Messaging)

EIM is an Instant Messaging Service that runs on private servers in a company on platforms such as the Live Communications Server.

Enterasys Switches

Enterasys switches are produced by Enterasys Networks as secure network solutions. The stackable switches support QoS features and can classify and prioritize voice, video and data applications.

ESP (Encapsulating Security Payload)

ESP is an IPsec protocol that guarantees packet encryption, packet integrity as well as packet authenticity. The integrity and authentication check does not extend to the IP header. It is only performed for the actual data (payload).

FoIP (Fax over IP)

FoIP is a method for transmitting fax messages over an IP network.

FTP

The File Transfer Protocol (FTP) is a network protocol specified in RFC 959 for the transmission of data via TCP/IP networks.

Functional Numbers

Functional numbers (also called function codes) are MSN/DID numbers or pilot numbers, e.g., for parking, conferencing and the AutoAttendant. The functional numbers correspond to virtual stations. The functional numbers in an internetwork must be unique.

G.711

G.711 is a standard for digitizing analog audio signals. It is used in classic fixed-network telephony (PCM technology). G.711 can also be used for voice encoding in VoIP.

G.729AB

G.729 is a codec for voice compression in digital signals and is used in IP telephony. G.729 is very CPU-intensive. Though only marginally inferior in terms of quality, G.729AB is a somewhat simplified version and therefore less CPU-intensive.

Gateway / Gateway Modules

A gateway is the entrance and exit to a communications network, usually connecting two disparate traffic flows.

GSM (Global System for Mobile Communications)

GSM is a standard for digital mobile networks that is primarily used for telephony, but also for line- and packet-switched data transmissions as well as short messages (SMS).

Handover

The term handover designates the process in a mobile cellular communication network in which the mobile phone switches from one cell to another during a call or a data connection. The term is also used when switching between GSM and UMTS with a dual-mode mobile phone.

Hash value

Hash or dispersion range values are usually scalable values from a subset of natural numbers. A hash value is also referred to as a "fingerprint" because it is a virtually unique identification of a quantity in much the same way as a fingerprint is a virtually unique identification of a person.

H.323

H.323 designates a group of standards that define a variety of media types for packet networks. The standards cover voice, data, fax and video, and define how signals are to be converted from analog to digital and what signaling is to be used.

OpenScape Business Assistant

OpenScape Business Assistant is used to administer the communication system. It provides all wizards for the quick support of administration tasks.

Hosted Services

Hosted Services are traditional IT services such as e-mail, instant messaging (IM) and unified communications (UC), which are provided to a company by an Internet Provider from a remote site, thus eliminating the company's need to run and manage these services on their own servers on-site.

ICMP (Internet Control Message Protocol)

ICMP is used in data networks for the exchange of information and error messages using the Internet Protocol IP.

IDS (Intrusion Detection System)

IDS is a security system that monitors all incoming and outgoing network activities to identify possible security violations. These include both intrusion (attacks from outside the organization) and abuse (attacks from within the organization).

IEEE Standards

IEEE Standards are a set of specifications defined by the Institute of Electrical and Electronic Engineers (IEEE) (such as Token Ring, Ethernet) to establish common networking standards among vendors.

IEEE. 802.1p

IEEE. 802.1p is an IEEE standard for regulating the transport of data packets with different priorities in computer networks. The data packets are classified into priority classes from 1 to 7. The Standard only stipulates ascending priorities from 1 through 7, but does not deal with how the individual data packets should be handled.

IKE Protocol

The IKE protocol has two different tasks. Start by creating an SA (Security Association) exclusively used by the IKE protocol (IKE-SA). The existing IKE-SA is then used for secure negotiation of all further SAs (payload SA) for the transmission of payload data.

IM (Instant Messaging)

IM is a procedure for the real-time exchange of text messages over the Internet using computers, Pocket PCs and mobile phones. Modern IM services enable VoIP and video conferencing, file transfers and desktop application sharing.

IP PBX

IP PBX is a communication system that supports both VoIP and normal voice connections over traditional phone lines.

IPSec

IPSec is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of various security services and protocols.

ISP (Internet Service Provider)

An ISP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations. Some ISPs are large national or multinational corporations that offer access in many locations, while others are limited to a single city or region.

ITSP (Internet Telephony Service Provider)

An ITSP is a business that supplies Internet connectivity services to individuals, businesses, and other organizations.

DP (Dial Pulsing)

DP is the oldest signaling method used for automatic telephone switching. Today, DP has generally been superseded by DTMF.

Jitter

Jitter refers to packet delay variations in voice transmissions. An excessive delay between the sending of packets and their arrival at the receiving end results in irregular voice communications infectivity are difficult to understand.

ISD (Individual Speed Dialing)

Individual Speed Dialing (ISD) enables 10 external individual speed-dial numbers to be saved at every authorized phone in addition to the system speed dialing (SSD).

SSD - System Speed Dialing

Frequently required external phone numbers can be stored in the system memory of the communication system. Every number is represented by a speed-dial number, which can be used instead of the full phone number by all stations.

Latency

Latency is the time required to transport a data packet from one application to another, including the time for transmission over the network and for preparing and processing the data at the transmitting and receiving devices.

LCR (Least Cost Routing)

You can use the Least Cost Routing (LCR) function to specify the provider you want to use, e.g., for trunk calls, mobile phone calls or international calls. You use the communication system to define the least-cost provider and conduct all calls via this specific path.

LIN (Location Identification Number)

LIN is an unique, max. 16-digit number that corresponds to the 10-digit NANP (North American Numbering Plan).

LWCA (Lightweight CA)

LWCA is a restricted certification function.

Media Stream Channel

A media gateway can terminate circuit-switched ISDN B channels and use the voice data carried to generate media stream channels for an IP-based packet-switched network. Media stream channels feature a combination of audio, video, and T.120 media.

DTMF (Dual Tone Multifrequency)

Dual Tone Multifrequency (DTMF) is the dialing method in analog telephony that is predominantly used in switching technology today for transmitting the phone number to the telephone network.

MIM (Mobile Instant Messaging)

MIM is a Presence and Instant Messaging Service for mobile phones.

Mobility

The term mobility designates the use of Pocket PCs and mobile phones and their integration in the communication system of a company.

MOH (Music on Hold)

Music on Hold (MOH) can be played to callers who cannot be switched through immediately.

MSN (Multiple Subscriber Number)

When connecting ISDN phones via an S0 bus (point-to-multipoint connections), every single ISDN phone (ISDN station) is assigned a unique Multiple Subscriber Number (MSN). The ISDN stations can be reached via their MSNs.

MULAP (Multiple Line Appearance)

MULAPs are special groups in which multiple telephones are combined. A group member may be assigned multiple phones under a single call number (Basic MULAP) here. In addition, such a group can be used to implement special features required for communication between an Executive and Secretary, for example, or within teams (Executive MULAP, Team MULAP).

Multi-Gateway

In the case of a multi-gateway network, calls are routed via several different gateways.

myAttendant

myAttendant is the attendant console of the communication system.

myPortal

myPortal is the Java-based user portal that enables subscribers to access the Unified Communications functions. Apart from information on the presence status, convenient dialing aid via favorites and directories, subscribers can also access voicemail messages and faxes.

myPortal for Outlook

myPortal for Outlook is the user portal integrated in Microsoft Outlook that enables subscribers to access unified communications functions. It is analogous to myPortal. myPortal for Outlook also provides a convenient Desktop Dialer.

NAC (Network Admission Control)

NAC is a technology that supports defenses against viruses and worms from within the network. With NAC, terminal devices are checked for conformity with guidelines during the authentication. If the virus scanner is not up-to-date, for example, or if the client operating system does not have the latest security patch installed, the device involved is quarantined and provided with the current updates until it meets the applicable security guidelines.

NAT (Network Address Translation)

NAT is a procedure for replacing one IP address in a data packet with another. It is used to map private IP addresses to public IP addresses. Masking or PAT (Port Address Translation) is when the port numbers are also rewritten.

NTBA (Network Termination for ISDN Basic Access)

An NTBA (Network Termination for ISDN Basic Access), also known as NT (Network Termination), is the network termination device for the ISDN basic rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

NTPM (Network Termination for Primary Rate Multiplex Access)

An NTPM (Network Termination for Primary Rate Multiplex Access) is the network termination device for the ISDN primary rate interface. It is the link between the network operator's digital network and the ISDN configurations on the subscriber side.

OLSR - Optimized Link State Routing Protocol

OLSR is special ad-hoc protocol that enables the missing routing capability on the OSI Layer 2 to be optimized on the OSI Layer 3.

ONS (One Number Service)

Call number directly assigned to a user One or more resources (telephones) may be assigned to a user. When a user is called via his or her ONS number, the call is forwarded to the phone that is currently being used by that user (e.g., a mobile phone).

PAP (Password Authentication Protocol)

PAP is an authentication procedure based on the point-to-point protocol. It is used for dialing into an ISP. PAP transmits the password for authentication as clear text together with a user ID.

PBX (Public Branch Exchange)

A PBX is a switching system that interconnects multiple terminals such as phones, fax and answering machines between themselves and also to the public phone network.

Peer

A peer is the terminal device for communication in a peer-to-peer network. During communication, every peer makes its services available and uses the services of the other peer.

Peer-to-peer

In a peer-to-peer network, all PCs have equal rights and may use and also provide services on the network.

Peer-entity authentication

The corroboration that the peer entity in an association is the one claimed.

PKI (Public Key Infrastructure)

In cryptology, a PKI (public key infrastructure) is a system for generating, distributing, and verifying digital certificates. The certificates issued within a PKI are used to protect computer-driven communication.

PPP (Point-to-Point Protocol)

PPP is an IETF standard for transmitting IP packets over serial lines. PPP is mainly used for dialing into the Internet.

PPPoE (Point-to-Point Protocol over Ethernet)

The PPPoE Protocol (PPP over Ethernet) enables the use of the Point-to-Point network protocol over an Ethernet connection.

Pre-shared Key

The pre-shared key is a key that is defined for the tunnel configuration (for VPNs). In order for VPN peers communicating via the tunnel to authenticate themselves, the same password must be used for both of the tunnel endpoints.

PPTP (Point-to-Point Tunneling Protocol)

PPTP is a technology used for configuring a virtual private network (VPN). Because the Internet is essentially an open network, PPTP is used to ensure that messages transmitted from one VPN node to another are secure. PPTP lets users dial into their corporate network via the Internet.

Presence

The term Presence refers to the capability of a Unified Communications system to determine the location and status of a user at any time. This makes it easier

to respond to the specific communication needs of a user by phone, e-mail, Instant Messaging or fax.

Proxy Server

The proxy server is the connecting link between a client application and a Web server. It performs the task of filtering client application requests and thus relieves the load on the Web server.

PSTN (Public Switched Telephone Network)

As the name implies, PSTN refers to a public switched telephone network. Public networks may be owned by private or public entities.

QoS (Quality of Service)

You must guarantee a minimum bandwidth for Voice over IP for the entire transmission duration. If multiple applications with equal rights are operating via IP, then the available bandwidth for a transmission path is split. In this case, a voice connection may experience packet losses which can reduce voice quality. There are different ways to guarantee the highest possible quality for transmission; these methods are collectively referred to as Quality of Service (QoS).

RAS (Remote Access Service)

A RAS (Remote Access Service) user is an IP subscriber (e.g., a teleworker) who logs into the system remotely and behaves like an internal IP station. This subscriber can therefore use the complete functional scope of the communication system.

RJ45 (Registered Jack 45)

RJ45 is an eight-pin connector that is used for connecting a 10BaseT cable in network technology, for example.

Roaming

Roaming is the capability of a mobile network subscriber to automatically make calls or access other mobile network services in a foreign network, i.e., one that differs from the home network of the subscriber.

RTCP (Real-Time Control Protocol)

The real time control protocol (RTCP) is used for the negotiation and compliance of Quality of Service (QoS) parameters through the periodic exchange of control messages between senders and receivers.

RTP (Real-Time Transport Protocol)

RTP is an IETF Standard for streaming real-time multimedia data using the Internet Protocol. Typically, RTP runs on top of the UDP protocol, and uses dynamic UDP ports negotiated between the sender and receiver of specific media streams.

RTT (Round Trip Time)

RTT is the time interval required by a data packet to move from the source to the target and back.

SA (Security Association)

SA is a security association between two communicating units in computer networks. It describes how the two parties will use security services to communicate securely with each other.

SDSL (Symmetric Digital Subscriber Line)

SDSL is particularly suited to Internet telephony, intranet applications in companies with local networks, for video conferencing and is, for example, designed for teleworkers who can use it to send and receive data with the same bandwidth. In contrast to ADSL, SDSL uses identical bandwidths from and to the Internet.

Secure CLI

Secure CLI is a security feature that provides secure command line and data transfer interfaces with the help of the Secure File Transfer Protocol (SFTP).

SFTP (Secure File Transfer Protocol)

SFTP is a security protocol for transporting connection data records.

ShrewSoft VPN Client

The ShrewSoft VPN client is an open source and free VPN client with a graphical user interface. It includes, among other things, ISAKMP, Xauth and RSA support, and AES, Blowfish and 3DES encryption protocols.

Single Gateway

In the case of a single-gateway network, calls are routed via a single gateway.

SIP (Session Initiation Protocol)

SIP is a standard Internet protocol defined in RFC 3261 for setting up and managing voice connections and video conferences over an IP network.

SNMP (Simple Network Management Protocol)

SNMP is a procedure for obtaining information on the status of network components and PCs.

SPE (Signaling and Payload Encryption)

Signaling & Payload Encryption (SPE) serves to enhance security when transmitting voice data. The VoIP payload and signaling data streams from and to the gateway and between IP phones are encrypted.

SRTP (Secure Real-Time Transport Protocol)

SRTP is an encrypted RTP protocol. It is particularly suitable for transmitting communication data over the Internet and is used in IP telephony.

SSH (Secure Shell)

SSH is a protocol that provides support for secure remote login, secure file transfer, and secure TCP/IP forwarding. It can automatically encrypt, authenticate, and compress transmitted data.

SSL (Secure Socket Layer)

SSL is a protocol for transporting documents over the Internet. With SSL, data is provided with a private key before it is transmitted. By convention, URLs that require an SSL connection start with https: instead of http:.

Status

The status, together with the "Presence" concept, indicates whether a subscriber is available, busy, offline, etc., so that other subscribers in the communication system know if this subscriber can be reached.

STUN (Simple Traversal of UDP through NAT)

STUN is a network protocol for detecting, identifying, and bypassing firewalls and NAT routers.

Survivability

Survivability is the capability of an internetwork to maintain service continuity in the presence of faults within the network.

TAE (Telekommunikations-Anschluss-Einheit) - German standard for telephone plugs and sockets

A TAE is a type of connector for analog phone connections with the a/b interface and for ISDN connections to plug the NTBA into the main line. It is used to connect analog telephones, fax machines and ISDN phone systems.

TCP (Transmission Control Protocol)

TCP is a protocol that governs how data should be exchanged by PCs. All operating systems in modern PCs support TCP and use it for data exchange with other PCs.

TFTP (Trivial File Transfer Protocol)

TFTP is a trivial file transfer protocol that supports only the reading and writing of files. Many of the functions supported by the superordinate protocol are unavailable, for example, functions allocating rights, displaying existing files or user authentication.

Telnet

A protocol that links two PCs in order to provide a terminal connection to the remote PC. Instead of dialing into the PC, the user connects over the Internet via Telnet. The user initiates a Telnet session, connects to the Telnet host and logs in. The connection enables the user to work with the remote PC as though it were a terminal connected to it.

TOS (Type of Service)

TOS is a field in the header of IP data packets. It is used for the prioritization of these packets and evaluated for Quality of Service, for example.

UCD (Uniform Call Distribution)

UCD enables incoming calls in the communication system to be uniformly distributed to a group of stations (UCD-group).

UDP (User Datagram Protocol)

UDP is a network protocol that belongs to the Transport layer of the Internet protocol family. UDP is responsible for routing data transmitted over the Internet to the correct application.

UMTS (Universal Mobile Telecommunications System)

UMTS is a third-generation mobile network standard with which significantly higher data transmission rates (384 kbps to 7.2 Mbit/sec.) can be achieved as compared to the mobile network standards of the second generation or the GSM standard.

Unified Communications

Unified Communications is the integration of various communication systems, media, devices and applications within an environment (e.g., IP telephony, site-based and mobile telephony, e-mail, instant messaging, desktop applications, voicemail, fax, conferencing and unified messaging).

Unified Messaging

Unified Messaging is the integration of different communication data such as e-mail, SMS, fax, telephony, etc., in a uniform message store. This message store can be accessed by several different devices.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) is an algorithm in speech processing to detect the presence or absence of speech in the digital transmission of audio data.

VCAPI Interface

VCAPI is a virtual CAPI interface that emulates the presence of a local ISDN card. If an ISDN card has been installed on a PC in the internal network, then this ISDN card can be made available to all stations on the network via the VCAPI interface.

VDSL (Very High Speed Digital Subscriber Line)

VDSL is used to transfer symmetrical or asymmetrical data streams at high speed over short distances. VDSL is an alternative to ADSL and SDSL that additionally offers higher transmission speeds.

VoIP (Voice over IP)

VoIP is the transmission of voice data over IP-based networks.

VPN (Virtual Private Network)

A VPN uses the public infrastructure of the Internet to connect sites and provide teleworkers with access to internal networks. External partners are provided with secure access to the internal data network by using encryption and authentication mechanisms.

WAN (Wide Area Network)

WAN is the designation for wide area data networks such as the Internet, for example.

WBM (Web-Based Management)

WBM is a web-based user interface that is displayed in an Internet browser using HTML or JAVA pages (web pages) and a web protocol (HTTP or HTTPS).

X.509 standard (VPN certificate)

X.509 is an ITU-T standard for a public key infrastructure and currently the most important standard for digital certificates.

XMPP (Extensible Messaging and Presence Protocol)

Internet standard that is primarily used for Instant Messaging. XMPP supports the interaction with users of other networks such as AIM, ICQ or Windows Live Messenger (WLM), for example. Among other things, XMPP and its extensions support conferencing with multiple users (e.g., multi-user chats) and the display of the online status.

Second Degree

Second degree means that a station is calling and already has a second call waiting for that station.

Index

A

accidents, reporting 78
Actions
  Automatic Actions, Expert mode 1442, 1443
  Manual Actions, Expert mode 1440
Actions, Expert mode 1440
activate licenses 299, 308
activation, software (see software activation) 1188
Active Certificates, Expert mode 1493
Active Directory Integration Service
  configure 1132
Active Directory Integration Service, Expert mode 1646
Active Directory Service 1131
Active Rules, Expert mode 1504
Active Services, Expert mode 1496
Active Tunnels, Expert mode 1497
ad-hoc conference 499, 568
Address Resolution Protocol, Expert mode 1445
admin log
  change language 991
Admin log
  change language 948, 948, 949, 949
  load 991
Admin log (also called admin protocol) 991
Admin Log Data, Expert mode 1440
Admin Protocol
  Admin Log Data, Expert mode 1440
  Configuration, Expert mode 1440
Admin Protocol, Expert mode 1439
advisory messages 639
AF/EF code points 415
alarm signaling, Expert mode 1435
All Leases, Expert mode 1522
Allowed lists
  display 726
Allowed Lists, Expert mode 1624
alternative workplace 534
Analog Stations, Expert mode 1568
analog telephone 426
announcement player 1679
announcement player, Expert mode 1480
announcements for call distribution 718
announcements for voicemail 578
answering machine 426
Application Diagnostics
  Developer Settings, Expert mode 1444, 1444
  Mainboard, Expert mode 1444
Application Diagnostics, Expert mode 1444
Application Firewall, Expert mode 1485
Application Launcher 1133, 1679
  profile for configuration data 1134
Application Launcher, Expert mode 1679
Application Selection 1645
application-controlled conference 498, 563
Applications, Expert mode 1645, 1679
Assign MSN, Expert mode 1621
audio codec 411
  assign parameters to a destination 413
  configure parameters 412
audio file 1173, 1175
authentication
  conference participant 499
AutoAttendant 577
Autom. night service, Expert mode 1628
automatic action 1214
  DLS notification 1216
  edit DLS notification 1216
  edit garbage collection 1214
  garbage collection 1214
  start DLS notification 728, 728, 729, 1217, 1219, 1220, 1221
  start garbage collection 1215
  stop DLS notification 1218
  stop garbage collection 1216
automatic callback 636
automatic recall 621
automatic updates 522
automatic wake-up system 647
Auxiliary Equipment
  Music On Hold, Expert mode 1629
  SmartVM, Expert mode 1633
Auxiliary Equipment, Expert mode 1592

B

back up 1179
backup 1179
  immediate 1184
  scheduled 1186
backup - immediate 1185
backup directory 1180
backup medium 1179, 1181
  add 1182
  delete 1184
  edit 1183
backup set 1179, 1180, 1180
  display 1181, 1181
  immediate backup 1185
  restore 1187
  scheduled backup 1186
backup set for diagnostic purposes 1274, 1275
bandwidths in the LAN 1003
Base stations, Expert mode 1417, 1417, 1570, 1596
Basic MULAP 690
  add 696, 700
  add a member 697

delete 697
delete a member 697
display 696
edit 696
edit a member 698
ring type 692
basic settings
power management, Expert mode 1483
Basic Settings 1446
announcement player, Expert mode 1480
Call Charges, Expert mode 1477, 1479, 1480
Date and Time, Expert mode 1475, 1475, 1475
DynDNS, Expert mode 1472, 1473
Gateway, Expert mode 1470, 1470
Phone Parameter Deployment, Expert mode 1481
Port Management, Expert mode 1476
Quality of Service, Expert mode 1474
System, Expert mode 1454, 1460, 1463, 1463, 1466, 1467, 1468, 1468, 1469
Basic Settings, Expert mode 1446, 1677
board status, Expert mode 1419
branding, Expert mode 1412
broadband connection 353

C

cable port 353
cabling for LAN and WAN connections 80
call
missed 557
scheduled 557
Call Charges - Account Codes, Expert mode 1480
Call Charges - Factors, Expert mode 1479
Call Charges - Output Format, Expert mode 1477
call deflection after timeout 631
call distribution 708, 709
accept UCD calls automatically 714
accept UCD calls automatically, activate 714
accept UCD calls automatically, deactivate 714
add a UCD agent 712
AICC (Automatic Incoming Call Connection) 714
announcements 718
change the overflow 717
configuration 708
configure 709
configure a UCD group 709
delete a UCD agent 712
edit a queue 715
edit announcements 718
edit Music On Hold (MOH) 718
edit the priority of external calls 714
edit the priority of internal calls 714
edit the wrapup time 713
night service 717
overflow 716
priority of external calls 713
priority of internal calls 713
queue 715
release UCD calls from analog lines 720
release UCD calls from analog lines, edit the release time 720
subscriber state 710
transfer to UCD group 719
transfer to UCD group, edit the recall time 719
UCD agent 710
UCD group 709
wrapup time 712
call forwarding 629
rule-based 535
status-based 535
call forwarding on busy 626
call forwarding-no answer after timeout 626
Call Forwarding, Expert mode 1607
call number format 497
call pickup from voicemail 578
call pickup group 651
activate warning tone 668
add member 661
call pickup for recalls 652
call pickup outside of a call pickup group 652
configure 660
deactivate warning tone 668
delete member 661
disable call pickup for recalls 669, 1007
disable the display of a caller's name 668
disable the display of a caller's phone number 668
display of a caller's name 651
display of a caller's phone number 652
enable call pickup for recalls 668, 1007
enable the display of a caller's name 668
enable the display of a caller's phone number 668
SIP phones 652
warning tone 652
Call Pickup, Expert mode 1604
call signaling 613
call supervision, Expert Mode 1427
call waiting tone/call waiting 636
call waiting/call waiting tone 636
callback 635
journal 557
callback on busy 636
Calling Line Identification Presentation - CLIP 614
Calling Line Identification Restriction - CLIR 615
CallMe 534
CallMe service 534
canonical call number format 497
capacities 1368
capacity limits 1368
Carrier Select Override 741
CCV objects 792, 840
CDP (Certificate Distribution Point) 982
CE Conformity 84
CE mark 82
Central License Server (see license server) 325

Certificate Generation, Expert mode 1507
Certificate Management, Expert mode 1493, 1508
Classes of Service
Allowed Lists, Expert mode 1624
Autom. night service, Expert mode 1628
CON Group Assignment, Expert mode 1626
CON Matrix, Expert mode 1627
Day
Class of Service Groups, Expert mode 1623
Denied Lists, Expert mode 1625, 1625
Night
Class of Service Groups, Expert mode 1624
Night service, Expert mode 1626
Special Days, Expert mode 1629
Stations, Expert mode 1622
Classes of Service, Expert mode 1622
Classes Of Service, Expert mode 1538
client (UC Smart) 468
client (UC Suite) 513
client logs 1283
download 1287
clients, hardware and software prerequisites 517, 803, 827, 831
CLIP - Calling Line Identification Presentation 614
CLIP no screening 616
clipboard dialer 559
CLIR - Calling Line Identification Restriction 615
CMD (CSTA Message Dispatcher) 1680
Codec Parameters, Expert mode 1541
collect call barring per trunk 738
COLP - Connected Line Identification Presentation 616
COLR - Connected Line Identification Restriction 616
communication system
shut down 1204
communication system, remote access 1299
Communities, Expert mode 1437
compliance
US and Canadian standards 84
CON Group Assignment, Expert mode 1626
CON groups 734, 735
allocation of SSD numbers 735
assign codes 736
assign subscribers/stations 736
CON matrix, edit 736
CON Matrix, Expert mode 1627
concept 69
condition
rule-based call forwarding 535
conference 499, 562, 571, 571
ad-hoc 568
application-controlled 562
authentication 562
automatic invitation by e-mail 562
automatic invitation via Outlook appointment 562
conference controller 562
conference participants 562
conference tone 562
dial-in number 562
extend 562
Mobility Entry stations 562, 568, 569, 572
open 572
phone-controlled 562
record 562
scheduled 569
types 562
virtual conference room 562
conference (UC Suite) 562
conference management 498, 563
conference tone, activate/deactivate 630, 630
conference, phone-controlled 498, 563
conferencing 571
Conferencing, Expert mode 1667
configuration
announcements, Expert mode 1408
branding, Expert mode 1412
IP gateway address, Expert mode 1412
SmartVM, Expert mode 1409, 1409, 1410
Configuration
Music on Hold (MoH), Expert mode 1407
Port Configuration, Expert mode 1408
configuration data 1179
configuration data for diagnostics 1274
generate 1275
Configuration, Expert mode 1407, 1440
configure call forwarding 506, 627
Configured Certificates, Expert mode 1494
Configured Rules, Expert mode 1505
Configured Services, Expert mode 1496
Configured Tunnels, Expert mode 1500
conformity
international standards 84
Connected Line Identification Presentation - COLP 616
Connected Line Identification Restriction - COLR 616
connection to central CLA;CLA
central connection 326
connection to local CLA;CLA
local connection 316, 317, 326
contact 557
contact center 825
Contact Center 791, 791, 792, 792, 840, 840, 840, 840
activate a queue 883
add a break 886
add a queue 877
add a schedule 871
agent 833
agent callback 849
assign agent to queue 890
break 835
class of service (authorization level) of an agent 833, 834
clients 825
conditions for operation 892
configure a UCD group 869
configure stations as agents 869

deactivate a queue 883
define preferred agents 886
define target values for the Grade Of Service 884
define the VIP caller priority 884
delete a break 887
delete a schedule 875
delete preferred agents 886
display queue details 849
download rule 876, 877
edit a break 887
edit a queue 881
edit a schedule 874
edit the VIP call list 885
fallback solution 850
Grade of Service 848
load announcement 871
multiple wrapup, add wrapup reason 889
multiple wrapup, delete wrapup reason 890
multiple wrapup, edit wrapup reason 889
myAgent 826
myReports 829
myReports user roles 829
predefined report templates 896
preferred agents 835
print rule 876, 876, 877
procedure for configuration 868
queue 838
record announcement 870
remove agent from queue 891
reports 895
restrictions on system features 893
save rule as PDF file 876
simple wrapup, add wrapup reason 888
simple wrapup, delete wrapup reason 888
simple wrapup, edit wrapup reasons 888
use of DECT phones 894
VIP call list 850
VIP caller priority 849
wallboard display 849
wrapup 848
wrapup reasons 848
Contact Center, Expert mode 1656
Contact Center:configuration 853
Contact Center:configuring a pilot for incoming Fax messages 883
Contact Center:example of a Contact Center configuration 853
cordless
system-wide, Expert mode 1592
Cordless
base stations, Expert mode 1596
Multi-SLC, Expert mode 1595
SLC, Expert mode 1594
Cordless phones 103
corporate network 748
cover page editor 587
CRL (Certificate Revocation List) 962
CRL(Certificate Revocation List) 982
CSP (CSTA Service Provider) 1680
CSTA Message Dispatcher (CMD) 1680
CSTA protocol 1104
CSTA Service Provider (CSP) 1680
CSV file 408
customer trace log 1246
delete 1255
display 1254
download 1255
edit 1254
open 1255
Customer Trace Log, Expert mode 1423

D

data backup (see backup) 1179
data protection 83
Data Protection 896
data security 83
Date and Time, Expert mode 1475
Day
Class of Service Groups, Expert mode 1623
DECT phones 103
DECT Stations, Expert mode 1571
default router 346
configure 347
Default Router, Expert mode 1525, 1527
defer a call 634
Denied list, display 726
Denied Lists, Expert mode 1625, 1625
departments 555
Departments, Expert mode 1652
Deployment and Licensing Client (DLSC), Expert mode 1486
Desk Sharing 914
desktop dialer 515, 559
Destination Codec Parameters, Expert mode 1543
Device Statistics, Expert mode 1640
Devices, Expert mode 1637
DHCP Mode, Expert mode 1517
DHCP relay agent:configure 338
diagnosis log 1269
delete 1274, 1274
download 1273
open 1273
diagnosis logs 1241
download 1244
Diagnosis Logs, Expert mode 1435, 1440
diagnosis protocol 1242
download 1244
dial pause 609
dial plan 131, 215, 406, 742
delete 409
edit 409
import 410
Dial Plan, Expert mode 1533

Dial Rule, Expert mode 1536
Dial-In Control Server 749
dial-in number
conference 499
dial-up network status 1207
check 1209
dialable call number format 497
DID Extensions, Expert mode 1588
digit dialing 603
digit transmission 740
select 741
digital loopback 1246
Digital Loopback, Expert mode 1423
digital signature 960
direct answering 611
Direct Station Select (DSS) key 610
directories (UC Smart) 487
Directories (UC Suite) 537
directory
instant message 502
DISA, Expert mode 1463
discreet call (whisper) 623
Display Conventions 69
Display, Expert mode 1460
disposal 79
DLI Maintenance, Expert mode 1442
DLS Notification, Expert mode 1443
DLSC CA Certificate, Expert mode 1488
DLSC Client Certificate, Expert mode 1487
DNS (Domain Name Service)
define server 346
DNS name 367
DNS server 345
DNS Server, Expert mode 1526
Do Not Disturb 634
download (see update) 1188
DSL (Digital Subscriber Line) 353
DSP channels, planning 1688
DSS key 610
DSS server 1681
dual-mode telephony 908
DynDNS 344
DynDNS (Dynamic Domain Name Service) 367
DynDNS service 367
configure 368, 386, 387, 387, 388, 937
DynDNS Service, Expert mode 1472

E

e-mail
notification 510, 589
e-mail settings 1269
e-mail to SMS 591
E-mail, Expert mode 1434
e-mail, send 590
E.164 numbering 1006
E911 emergency call service 777
edit a phone number 604
electrical environment
OpenScape Business S 80
OpenScape Business UC Booster Server 80
electromagnetic interference 82
email
invitation to conference 499
emergency calls
prerequisites 773
emergency, what to do 78, 78
en-bloc dialing 603
entrance telephone/door opener 1097
ESP header 951
Euro-ISDN features 1684
event 1268, 1268, 1268, 1269, 1269
change e-mail settings 1271
clear log 1270
display reaction table 1271
download log 1270
edit event logging via a LAN 1270
edit reaction settings for an event 1272
edit reaction settings for multiple events 1272
Event Configuration, Expert mode 1433
Event Log, Expert mode 1433
event viewer 1246
clear the event log 1255
display the event log 1254
download the event log 1255
edit the event log 1254
open the event log 1255
events
alarm signaling, Expert mode 1435
Events
Diagnosis Logs, Expert mode 1435
E-mail, Expert mode 1434
Event Configuration, Expert mode 1433
Event Log, Expert mode 1433
Reaction Table, Expert mode 1434
Events, Expert mode 1433
EVM, Expert mode 1572
exception
rule-based call forwarding 535
Executive function (see Executive/Secretary configuration) 676
Executive MULAP 693
add 698
add a member 699
delete 699
delete a member 700
display 699
edit 699
edit a member 700
ring type 694
SIP phones 695
Executive/Secretary (see Executive/Secretary configuration) 676
Executive/Secretary configuration 676
add 683

add a fax box 690
add a member 688
delete 685
delete a member 688
edit 684
edit a member 689
edit the properties of a member 689
fax box 678
ring type 678
SIP phones 679
Expert mode, Expert mode 1406
external call forwarding - no answer 631
external directory 541
external directory (LDAP) 545
External Directory, Expert mode 1654
External Providers Config, Expert mode 1655

F

FastViewer 500, 573, 573
favorites list 557
instant message 502
favorites list (UC Smart) 490
fax 578
T.38 594
fax box 585
fax box group 702
add a member 706
configure 705, 706
delete a member 706
display 706
edit 706
fax group (see fax box group) 702
Fax Group 3 426
Fax Group 4 423
fax headlines, Expert mode 1676
fax messages 578, 818
Fax Printer 515, 586
features
voice, network-wide 1002
File Upload, Expert mode 1666
fire safety requirements 81
firewall 938, 1134
fixed call forwarding 626
Flex Call 643
Flexible Menus, Expert mode 1468
Forwarding, Expert mode 1643
FTP Server, Expert mode 1517
function keys 427
program 428, 466, 467, 468, 486, 486, 510
functions
myPortal 514
myPortal for Outlook 515
myPortal Smart 470

G

Garbage Collection, Expert mode 1442
Gateway, Expert mode 1470
Gigaset phones 103
Global Parameter, Expert mode 1518
group call 653
disable DND for group members 671
DND for group member 653
enable DND for group members 671
of type call waiting, add 669
of type call waiting, add a member 670
of type call waiting, delete 670
of type call waiting, delete a member 670
of type call waiting, display 670
of type call waiting, edit 670
of type group, add 661
of type group, add a member 664
of type group, delete 663
of type group, delete a member 664
of type group, edit 662
of type RNA (ring no answer), add 669
of type RNA (ring no answer), add a member 670
of type RNA (ring no answer), delete 670
of type RNA (ring no answer), delete a member 670
of type RNA (ring no answer), display 670
of type RNA (ring no answer), edit 670
ring type 655
SIP phones 656
voicemail box 654
Group Members, Expert mode 1600
groups 651
Groups, Expert mode 1652
Groups/Hunt groups, Expert mode 1596

H

H.323 stack trace
clear log 1259
display the configuration 1258
download log 1259
edit modules 1259
edit the configuration 1258
open log 1259
H.323 Stack Trace 1248
H.323 Stack Trace, Expert mode 1426
hardware configuration of OpenScape Office MX
display 463
hardware, replace 323
hold 618
holiday schedule 791, 840
Host Name, Expert mode 1510, 1523
Hot Desking 914
hoteling 644
hotline 774
hotline after timeout 774

hunt group 656
add 664
add a member 667
delete 666
delete a member 667
edit 665
ring type 659
SIP phones 659
voicemail 657
HW Modules, Expert mode 1638

I

ICMP (Internet Control Message Protocol) 1228
IKE SA 960
IM (instant message) 502
image file 1188
Incoming Calls
Call Forwarding, Expert mode 1607
Call Pickup, Expert mode 1604
Group Members, Expert mode 1600
Groups/Hunt groups, Expert mode 1596
Team/top, Expert mode 1601
UCD, Expert mode 1605
Incoming Calls, Expert mode 1596
Individual Speed Dialing (ISD) 609
initiating a restart of OpenScape Business 1201
installation 128, 211, 263
instant message 502, 502, 502, 576, 576, 576
instant messages 818
instant messaging 576, 818
Intercept/Attendant/Hotline, Expert mode 1463
internal directory (UC Smart) 489
internal directory (UC Suite) 539
internal Music On Hold 1173, 1175
internal paging 707, 707
transfer call 708
Internet access 353
configuration 354
configure via a preconfigured ISP 360
configure via the standard ISP PPPoE 363
configure via the standard ISP PPTP 365
via an external Internet modem 359
via an external Internet router 355
Internet modem 359
Internet router 355
Internet telephony 370
Internet Telephony Service Provider (ITSP) 173, 234, 370, 372
Internet Telephony Service Provider, Expert mode 1544
inventory management 1207
inventory of OpenScape Office LX/HX
check 328, 328
inventory, OpenScape Business S 1211
check 1213
inventory, OpenScape Business X 1211
inventory, OpenScape Business X3/X5/X8
check 1212
invitation
conference 499
IP Address Pools, Expert mode 1519
IP address scheme 132, 214
IP addresses 1208
display an overview 1210
IP client (see IP stations) 417
IP Clients, Expert mode 1565, 1590
IP Diagnostics
Mainboard, Expert mode 1445, 1445, 1445
IP Diagnostics, Expert mode 1445
IP gateway address, Expert mode 1412
IP Mobility 914
IP stations 417
IPSec tunnel 959
ISDN card 423
ISDN modem 423
ISDN outside line
configure 390
ISDN parameters, Expert mode 1622
ISDN phone 423
ISDN stations 423
ISDN Stations, Expert mode 1569
ISDN trunk
selective seizure 749
ITSP (Internet Telephony Service Provider) 370
ITSP status 1208
check 1210

J

Java 1134
Java Runtime Environment (JRE) 129, 212
journal
retention period 557
journal (UC Smart) 497
journal (UC Suite) 557

K

Kernel Crash Data Service
start 1264
stop 1264
key combination for the Desktop Dialer 559
key programming 427, 427
Key Programming, Expert mode 1591
keypad dial 603

L

LAN 1 (WAN), Expert mode 1510
LAN 1, Expert mode 1523
LAN 2, Expert mode 1515, 1524
LAN 3 (Admin), Expert mode 1516
LAN requirements 1003

languages 104
Last active Leases, Expert mode 1522
LCR
Classes Of Service, Expert mode 1533
Dial Rule, Expert mode 1536
LCR flags, Expert mode 1533
Multisite, Expert mode 1538
Plan, Expert mode 1533
Routing Table, Expert mode 1534
LCR (Least Cost Routing) 738
assign/change Class of Service 745
class of service 745
dial plan 742
edit the dial plan 743
edit the outdial rules 748
edit the routing table 744
functionality 739, 739
outdial rules 746
routing table 744
LCR flags, Expert mode 1533
LDAP connection 1134
LDAP, Expert mode 1466
license 285
activate via a license file 301
activate via license authorization code 300, 1343
display information 318, 318, 319, 320, 320, 328
update 324
License Authorization Code (LAC) 299, 308
license component trace 1249
edit 1260
License Component trace, Expert mode 1429
license file 299, 308
license server (CLS) 303, 325
edit the IP address 200, 250, 306, 314, 316, 321, 322, 322, 323, 325
licensing procedure 307
lightning protection requirements 81
Lightweight CA 961
Lightweight CA, Expert mode 1492
live call recording (voice recording) 624
load to gateway, Expert mode 1408
Load to Gateway, Expert mode 1407
locking the phone 737
log entries 1268
log file 1268
loudspeaker 426
LXV3, Expert mode 1678

M

M5T trace component 1246
display 1256
edit 1256
start 1256
stop 1256
M5T Trace Components, Expert mode 1424
Mail Exchange entry 367
Mail Exchanger 367, 367
define 369
Mainboard, Expert mode 1444, 1518
Maintenance, Expert mode 1407, 1678
Manager E 125
manual action 1241
mapping (presence status, UC Suite) 532
maximum values
features 1376
MCL Single Stage 748
MCL Two-Stage 748
MEB (Media Extension Bridge) 1681
Media Extension Bridge (MEB) 1681
Media Server Trace
start 1265
stop 1265
Media Server Traces, Expert mode 1432
Media Stream Control (MSC), Expert mode 1637
Mediatrix 4102S 103
medium, backup (see backup medium) 1181
message overview 817
message texts 640
messages
manage 817
min network supplier 748
mobile logon 914
mobile PIN 644
mobile user logon 914
mobility
configure mobile phones for GSM 909
delete a station 913
Mobility Clients, Expert mode 1588
Mobility Entry 902
feature codes 903
Mobility Entry stations 571, 571
conferencing 499, 562, 568, 569, 572
modem 426
MoH 1173, 1175
MSC Statistics, Expert mode 1641
multi-location 997
Multi-SLC, Expert mode 1595
multilingual text output 1172
music on hold 1173, 1175
Music On Hold (MOH) 718
Music On Hold (MOH) for call distribution 718
Music on Hold, Expert mode 1629
MX record 367
myAgent
prerequisites 827
myPortal
functions 514
presence status 514
myPortal for Outlook
functions 515
myPortal Smart
functions 470
myPortal to go
prerequisites 901

myReports
reset administrator password 830
user roles 829

N

NAT (Network Address Translation) 941
NAT rule
configure 941
configure with NAT table editor 942
delete 943
NAT rules 941
NAT table editor 942
NAT, Expert mode 1527
Native SIP Server Trunk, Expert mode 1557
NCP client
activate, deactivate 969
provisioning 969
network
heterogeneous, hybrid 996
homogeneous, native 996
license 1002
network carriers 748
network connection check
ping 1228
using traceroute 1228
network connection, check 1228
Network Interfaces 1518
Application Board, Expert mode 1523, 1523, 1524
Expert mode 1510
Mainboard, Expert mode 1510, 1510, 1515, 1516, 1517, 1517, 1519, 1521, 1522, 1522
network parameters (LAN, WAN) 1002
network plan 996
networking
remove nodes from internetwork 1090
Night
Class of Service Groups, Expert mode 1624
Night Service, Expert mode 1626
Nodes, Expert mode 1555
notes on using myAgent and UC Suite clients simultaneously 832
notification
fax message 589
voicemail 510, 589
notification service 510, 589
numbering
closed 1005
open 1005

O

Online User 1305
starting 1227, 1305
Online User, Expert mode 1446
Online Users 1446
open conference 572
Open Directory Service 1134
Basic Settings, Expert mode 1677
Data sources, Expert mode 1677, 1678, 1678
Maintenance, Expert mode 1678
Open Directory Service, Expert mode 1677, 1679
OpenScape Business Assistant 108, 110
OpenScape Business X3R
protective grounding 1339, 1340, 1342
OpenScape Business X5R
protective grounding 1339, 1340, 1342
OpenScape Office MX inventory
check 328
OpenScape Office, Expert mode 1677
OpenScape Personal Edition 103
OpenStage 103
OpenStage Attendant 801
operating conditions (environmental, mechanical)
OpenScape Business S 85
OpenScape Business UC Booster Server 85
OpenScape Business X3, X5, X8 85
operating instructions 69
optiPoint 103
Out of Service, Expert mode 1420
outdial rules 746
outside line
configure ISDN outside line 390
override 638

P

padding 952
parking 618
path optimization 1006
path replacement 1006
Payload
Devices, Expert mode 1637
HW Modules, Expert mode 1638
Media Stream Control (MSC), Expert mode 1637
payload SA 960
Payload, Expert mode 1637
PC clients 103
PDF file
fax message 585
notification 589
Peer Certificates, Expert mode 1495
permanent 571
permanent conference 499, 571
phone image
deploy to device, Expert mode 1416
Load, Expert mode 1415
phone images
Deploy, Expert mode 1415
phone lock, individual 737
phone logo
Load, Expert mode 1416
phone numbers
import 410
Phone Parameter Deployment, Expert mode 1480

PIN for activating a shutdown 1204
Ping, Expert mode 1445
PKI server
add 981
display 981
Platform Diagnostics, Expert mode 1444
port 1134
Port Configuration, Expert mode 1408
Port Management, Expert mode 1476
port/board status, Expert mode 1419
ports 939
configure port opening 939, 1087
port administration 940
power management, Expert mode 1483
power supply circuit and connection
OpenScape Business S 80
OpenScape Business UC Booster Server 80
PPP Log, Expert mode 1529
pre-shared keys 960
prerequisites for Application Launcher 1134
prerequisites for myAgent 827
prerequisites for myPortal to go 901
prerequisites for myReports 831
presence (UC Smart) 487
presence (UC Smart) 487
presence (UC Suite) 532, 532
presence status 514
call forwarding 535
Presence Status (UC Smart) 487
presence status (UC Suite) 532
prevention of speaker calls for stations
disabling 611
enabling 611
prevention of voice calling for stations 611
Primary Rate Interface 749
prioritization of outside lines (trunks) 404
priority classes 415
private trunk 613
profile with configuration data for Application Launcher 1134
profiles
add members 455
create new profile 453
delete members 455
display 454
display members 454
editing 457
export all profiles 458, 934
export single profile 456
import all profiles 458, 934
import single profile 456
subscribers 453
Profiles, Expert mode 1674
profiles:export all profiles 458, 934
profiles:import all profiles 458, 934
Profiles/Templates, Expert mode 1586
proper use of communication systems and servers 79
PSTN Peers, Expert mode 1529
PSTN, Expert mode 1528
Public Key Infrastructure (PKI), Expert mode 1506
public phone numbers in the network 1006

Q

QSIG Features, Expert mode 1620
Quality of Service (QoS) 415
configuring 417
Quality of Service, Expert mode 1533
Quality of Service, Expert Mode 1474

R

radio frequency interference 82
RAS user 417
reaction table 1269
Reaction Table, Expert mode 1434
Read Communities, Expert mode 1438
record 560
recycling 79
redialing 605
rejecting calls 634
reload of the UC Booster Card 1205
reloading OpenScape Business 1202
relocate 644
remote access 1299
configure PC with Windows 7 1302
disable 1304
enable via Internet access with a fixed IP address 198, 201, 201, 202, 248, 251, 251, 252, 1303
enable via Internet access without a fixed IP address 1303
enable via ISDN 1300
PC configuration 1300
remote services 1293
Restart / Reload
Restart / Reload, Expert mode 1436
Restart / Reload, Expert mode 1436, 1436
restarting OpenScape Business 1201
restore 1179, 1187
restore (see restore) 1187
ringing assignment 632
ringing group on 632
Route, Expert mode 1613
routes 389, 394
add direction prefix incoming 396, 400
assign codes 398
assign Names 398
configure number and type, outgoing 400
configure the call number type 400
enter a second CO code 401
enter an overflow route 398
enter PABX number 399
routing 346

Routing
IP Routing, Expert mode 1525, 1525, 1526, 1526, 1527
NAT, Expert mode 1527
PSTN, Expert mode 1528, 1529, 1529
routing table 744
Routing Table, Expert mode 1534
Routing, Expert mode 1525, 1555
RPCAP daemon 1267
disable 1267
enable 1267
rpcap Daemon, Expert mode 1431
rule 535
Rule editor 792, 840

S

safety information 70
safety information for Australia 74
safety information for Brazil 74
safety information for Canada 77
safety information for the U.S. 75
schedule 791, 840
scheduled conference 499, 569, 569
Schedules, Expert mode 1664
scope of the voicemail box 578
Secretary function (see Executive/Secretary configuration) 676
secure trace
change passphrase 1257
change password 1257
import certificate from X.509 file 1258
import X.509 file 1258
start 1257
stop 1257, 1257
Secure Trace 1247
Secure Trace Certificate, Expert mode 1425
Secure Trace Settings, Expert mode 1425
secure trace state
query status 1257
Secure Trace, Expert mode 1424
Security
Application Firewall, Expert mode 1485
Deployment and Licensing Client (DLSC), Expert mode 1486
Deployment- und Licensing Client (DLSC), Expert mode 1487, 1488
Signaling and Payload Encryption (SPE), Expert mode 1490, 1490, 1491
SQL Security, Expert mode 1510
SSL, Expert mode 1507, 1508, 1508
VPN, Expert mode 1491, 1492, 1493, 1493, 1494, 1495, 1496, 1496, 1497, 1500, 1504, 1505, 1506
Web Security, Expert mode 1509
Security Associations SA 959
security checklist 938
Security, Expert mode 1485
Server Certificates, Expert mode 1508
Server, Expert mode 1668
service codes, Expert mode 1469, 1469
services, block (only LX) 945
shutdown
PIN for activation 1204
shutdown of OpenScape Business X 1204
Signaling and Payload Encryption
activate SPE support 948
deactivate SPE support 948
Signaling and Payload Encryption (SPE) 946
Signaling and Payload Encryption (SPE), Expert mode 1490
single location 997
SIP client 417
SIP Interconnection, Expert mode 1555
SIP Parameters, Expert mode 1538
SIP Phones 103
Site List, Expert mode 1667
Site of Operations, Expert mode 1645
SLC, Expert mode 1594
SmartVM, Expert mode 1409, 1409, 1410, 1633
SMS
notification 589
SMS notification 591
SMS template 591
SNMP
Communities, Expert mode 1437, 1438, 1438, 1438
Traps, Expert mode 1439
SNMP (Simple Network Management Protocol) 1229
add a community 1239
communities 1229
delete a community 1240
display communities 1239
display trap details 1241
display traps 1240
edit a community 1239
Management Information Database (MIB) 1229
traps 1230
SNMP Statistics, Expert mode 1641
SNMP, Expert mode 1437
SNTP Settings, Expert mode 1475, 1475
software activation 1188
Software Image
System Software, Expert mode 1413, 1414, 1414
Software Image, Expert mode 1413, 1417
software transfer 1188
software update (see update) 1188
software updates 1188
SPE CA Certificates, Expert mode 1491
SPE Certificate, Expert mode 1490
speaker call 611
speaker call for groups 707
Special Days, Expert mode 1629
Speed dials, Expert mode 1678
Speed Dials, Expert mode 1468
SQL Security, Expert mode 1510

SSDP (Smart Services Delivery Platform) 1293
configure PIN for activating/deactivating the service plugin 1299
configure Service Plugin for customer network with proxy 1296
deactivate Service Plugin 1298
reset Service Plugin 1298
SSL (Secure Socket Layer) 981
activating a certificate 988
display certificates 944, 944, 945, 987
exporting a certificate 988
generating a CA certificate 983
generating a certificate request 985
generating a self-signed certificate 984
importing a server certificate 986, 987, 989
importing an updated certificate 988
removing a certificate 987
standards 1682
Static IP Addresses, Expert mode 1521
static routes 346
add 347, 350, 351, 352
delete 348
Static Routes, Expert mode 1525, 1526
Station 1562
Key Programming, Expert mode 1591
Stations, Expert mode 1565, 1568, 1569, 1570, 1571, 1572, 1573, 1586, 1588, 1588
station data
import 410
station flag
call waiting rejection on 671
prevention of voice calling off 611
Station Parameters, Expert mode 1574
station status 1207
stations 406
analog 426
configure with wizards 430
IP 417
ISDN 423
Station, Expert mode 1585
Stations
Overview, Expert mode 1590
Station, Expert mode 1574
Stations, Expert mode 1562, 1562, 1622, 1643
Statistics
Gateway Statics, Expert mode 1640
Gateway Statistics, Expert mode 1641
SNMP Statistics, Expert mode 1641
Telephony Statistics, Expert mode 1642, 1642, 1642, 1643, 1643
Statistics, Expert mode 1640
status of stations
check 1208
status of the communication system 1207
status-based voicemail announcements 578
STUN (Simple Traversal of UDP through NAT) 388
suffix dialing 606
survivability 1088
system client 417
system connection 1134
system directory 490
system directory (UC Suite) 547
system flag
call pickup after automatic recall 669, 1007
calling number in pick-up groups / ringing groups / CFN / RNA 668
SPE support 948
warning signal for call pickup groups 668
System Flags, Expert mode 1446
system language for voicemail 578
System Speed Dialing (SSD) 606
System Texts, Expert mode 1642
System-wide, Expert mode 1592
System, Expert mode 1446

T

T.38 Fax 594
Take Over Write Token, Expert mode 1444
TCP dump 1266
delete 1266
start 1266
stop 1266
TCP Dump, Expert mode 1430
team (see team configuration) 672
team configuration 672
add 680
add a fax box 688
add a member 686
change programmed feature keys 687
delete 682
delete a member 686
edit 681
edit members 686
edit the properties of a member 687
fax box 674
ring type 674
team function (see team configuration) 672
team group 672
add 680
add a fax box 688
add a member 686
change programmed feature keys 687
delete 682
delete a member 686
edit 682
edit members 686
edit the properties of a member 687
fax box 674
ring type 674
Team/top, Expert mode 1601
Telefon-Logo
Verteilen, Experten-Modus 1417
Telephones 103
Telephony, Expert mode 1446

teleworking 534, 929
Templates, Expert mode 1653
Terminal server and Citrix server environments 514
Texts, Expert mode 1467
TIFF file
  fax message 585
  notification 589
time parameters
  monitor a UCD call on an analog line 720
  monitor an unscreened transfer to a UCD group 719
Time Parameters, Expert mode 1454
timed reminder;appointment 647
toggle/connect 620
toll restriction 721
  add phone number to allowed list 725
  add phone number to Denied list 725
  configure 724, 724, 729, 731, 731
  display Allowed list 726
  display Denied list 726
  edit filter for Denied List 726
top group 676
  add 683
  add a fax box 690
  add a member 688
  delete 685
  delete a member 688
  edit 684
  edit members 689
  edit the properties of a member 689
  fax box 678
  ring type 678
  SIP phones 678
topics, types 69
trace 1244
  clear log 1251, 1252
  display output interfaces 1254
  display the format configuration 1254
  download log 1251
  edit output interfaces 1254
  edit the format configuration 1254
  log 1246
trace component 1250
  display 1261
  display details 1262
  edit 1263, 1263
  start 1262
  stop 1262
  stop all components 1262
Trace Components, Expert mode 1430
Trace Console Output, Expert mode 1444
Trace Format Configuration, Expert mode 1421
Trace Log, Expert mode 1423
Trace Output Interfaces, Expert mode 1422
trace profile 1249
  add 1261
  display 1252
  display details 1260
  start 1253
  stop 1253
  stop all profiles 1260
Trace Profiles, Expert mode 1429
trace:format configuration 1245
trace:output interfaces 1245
Traceroute, Expert mode 1445
traces
  call supervision, Expert mode 1427
Traces
  Customer Trace Log, Expert mode 1423
  Digital Loopback, Expert mode 1423
  H.323 Stack Trace, Expert mode 1426
  License Component, Expert mode 1429
  M5T Trace Components, Expert mode 1424
  Media Server Traces, Expert mode 1432
  rpcap Daemon, Expert mode 1431
  Secure Trace, Expert mode 1424, 1425, 1425
  TCP Dump, Expert mode 1430
  Trace Components, Expert mode 1430
  Trace Format Configuration, Expert mode 1421
  Trace Log, Expert mode 1423
  Trace Output Interfaces, Expert mode 1422
  Trace Profiles, Expert mode 1429
Traces, Expert mode 1421
transfer calls 620
transfer to group from announcement 708
transfer, software (see software transfer) 1188
translation of station numbers to names 618
transmission of customer-specific call number information 616
Trap Communities, Expert mode 1438
Traps, Expert mode 1439
trunk queuing 612
trunk release for emergency call 776
Trunk Status, Expert mode 1642
trunks 389
  assign MSNs 393
  change the protocol 393, 394, 394
  configure the type of seizure 399, 402, 404
  edit codes 392, 392, 393
  edit routes 397
  type of seizure 395
Trunks, Expert mode 1610
Trunks/Routing
  Assign MSN, Expert mode 1621
  ISDN parameters, Expert mode 1622
  QSIG Features, Expert mode 1620
  Route, Expert mode 1613
  Trunks, Expert mode 1610
Trunks/Routing, Expert mode 1610

U

UC Application
  restart 1206, 1206
UC Applications, Expert mode 1585

UC Booster Card
restart 1205, 1205
UC Smart
Basic Settings 1647
query status 1293
status 1292
Status 1648
User Management 1647
UC Smart Client 468
UC Smart, Expert mode 1646
UC Suite 1649
client logs 1283
Conferencing, Expert mode 1667
configure e-mail notifications for system errors 1289
configure retention period for contact center data 1292
configure retention period for log files 1291
configure storage path for client log files 1285
configure time for maintenance 1291
Contact Center, Expert mode 1656
Departments, Expert mode 1652
disable recording of system logs 1284
disable saving of client logs on system hard disk 1286
download client logs 1287
e-mail notification 1287
enable recording of system logs 1284
enable saving of client logs on system hard disk 1286
External Directory, Expert mode 1654
External Providers Config, Expert mode 1655
Fax Headlines, Expert mode 1676
File Upload, Expert mode 1666
Groups, Expert mode 1652
performing system maintenance immediately 1292
Profiles, Expert mode 1674
Schedules, Expert mode 1664
Server, Expert mode 1668
Site List, Expert mode 1667
Templates, Expert mode 1653
User Directory, Expert mode 1649
UC Suite
disable recording of client logs on station-specific basis 1285
disable recording of client logs on system-wide basis 1284
enable recording of client logs on station-specific basis 1285
enable recording of client logs on system-wide basis 1284
maintenance 1282, 1290
monitoring 1282
notification 1288
system logs 1283
UC Suite Clients 513
UC Suite, Expert mode 1649
UCD (Uniform Call Distribution) (see call distribution) 708
UCD Agents, Expert mode 1642
UCD, Expert mode 1605
UP0 Stations, Expert mode 1562
update 1188
custom 1196
update licenses 323
Update Timer DNS Names, Expert mode 1473
Update via File Upload, Expert mode 1414
Update via Internet, Expert mode 1413
Update via USB Stick, Expert mode 1414
update, full
start in the background 1194
start with progress indicator 1192, 1200
update, software (see software updates) 1188
upgrade 1188
user (station) profiles 453
user buttons 817
layout 817
User Directory, Expert mode 1649
user profiles for the UC Suite 528
users of UC Smart
edit data 486, 486, 510
users of UC Suite
change length of password 527
change password 527
change presence status 527
configure as agents 526
edit data 525
users of UC Suite 523
reset 526

V

virtual conference room 499
Virtual Stations, Expert mode 1573
Voice Gateway
Codec Parameters, Expert mode 1541
Destination Codec Parameters, Expert mode 1543
Internet Telephony Service Provider, Expert mode 1544
Networking, Expert mode 1555, 1555
SIP Interconnection, Expert mode 1555, 1557
SIP Parameters, Expert mode 1538
Voice Gateway, Expert mode 1538
voicemail 578
call pickup 578
save 578
status-based announcements 578
voicemail box 578
voicemail box (UC Smart) 503
voicemail box, see voicemail 578
voicemail group 701, 701
add 703
add a member 704
delete 704
delete a member 704
display 703
edit 703
edit members 704
voicemail messages 578, 818
voicemails (UC Smart) 503

VPN
authentication 960
bandwidths 951
clients 966
security mechanisms 959
VPN (Virtual Private Network) 950
end-to-site 950
site-to-site 950
VPN active services
display a special service 972
display all services 971
VPN active tunnels
display 974
display rules 974
VPN certificates 961
display 963
generating a certificate request 964, 965
generating a Lightweight CA certificate 962
import 965
importing a trusted CA certificate 964
VPN configured services
change 972
delete 973
display all services 972
rename 973
VPN configured tunnels
add 976
display 975
display rules 975
VPN rules
add a configured rule 979
add for opposite direction 980
delete 980
display a special active rule 978
display all active rules 977
display all configured rules 978
edit 979
VPN status 1208
VPN, Expert mode 1491

W

WAN 367
warnings 70
caution 72
danger 71
note 73
warning 71
WAV file
notification 510, 589
Wave file 1173, 1175
WBM 108
home page 108
web collaboration 500
Web Collaboration 573, 573, 573
Web Collaboration, Expert mode 1676
Web Security, Expert mode 1509
Web Services 1134
Web Collaboration, Expert mode 1676
Web Services Interface 1119
Web Services, Expert mode 1676
Web-Based Management 108
wizards 117
WLAN phones 104
Write Communities, Expert mode 1438

© 2026 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.