



A MITEL
PRODUCT
GUIDE

Mitel OpenScape UC Application V11

Configuration and Administration

Administrator Documentation

02/2026

Notices

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

Trademarks

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

© Copyright 2026, Mitel Networks Corporation

All rights reserved

Contents

1 History of Changes.....	18
2 About this Manual.....	19
2.1 Target Group of this Manual.....	19
2.2 This Manual's Content.....	20
2.3 Manual Structure.....	20
2.4 General Conventions.....	23
2.5 Representation Conventions.....	23
2.5.1 Text Markups.....	23
2.5.2 Further Markups.....	24
2.5.3 Representation of the Configuration Process – System Configuration.....	24
2.5.4 Markups for Configuration Steps which Are Subject to Restrictions.....	24
2.5.5 Representation of the Configuration Process – Certificate Strategy.....	25
2.6 Specified Deployment Scenarios.....	25
2.7 Specified Default Passwords.....	26
2.8 Acronyms used.....	26
2.9 Continuitive Documentation.....	28
2.10 Data Protection and Data Security.....	28
3 Features with individual Configuration.....	30
3.1 One-Number Service (ONS).....	30
3.1.1 Interworking with Multi-Line Hunt Group (MLHG).....	31
3.2 The Conference Portal.....	31
3.3 The Voice Portal.....	31
3.4 Microsoft Exchange Connection.....	32
3.5 IBM Lotus Domino Connection.....	33
3.6 LDAP Connection.....	35
3.7 Instant-Messaging Connection.....	35
3.8 OpenScape Xpressions Connection.....	36
3.8.1 OpenScape Xpressions Connection Overview.....	36
3.8.2 Working Method of the OpenScape Xpressions Connection.....	36
3.8.3 Calling Number Schema.....	37
3.8.4 Restrictions on the OpenScape Xpressions Connection.....	40
3.8.5 Simultaneous availability of WebAssistant and the Voice Mail tab in WebClient.....	40
3.9 Networking Deployment Scenarios.....	41
3.10 Proxy-based Login.....	41
3.11 Presence Status in VCard.....	42
3.12 Outlook contact picture is not shown in UC.....	42
3.13 Using Chat History.....	42
3.14 Outlook Extension / Fusion for Office - add Grace period for calendar.....	43
3.15 Voicemail tab for UC WebClient and Fusion for Office / Notes.....	44
3.16 New Voice Mail Greeting Feature (UCMODE).....	44
3.16.1 New Voice mail Greetings Activation in WebClient and Fusion for Office.....	46
3.16.2 UC Voice mail modes.....	46
3.16.2.1 How to change to new Voice mail Greetings mode.....	46
3.16.2.2 How to change the user profile to 'Default system settings' for all users' voicemail boxes:.....	47
3.16.2.3 Default Mode (UCMODE = X).....	47
3.16.2.4 New Greetings Mode (UCMODE = U).....	48
3.16.2.5 OpenScape Xpressions Mode with the option to change to New greetings mode (UCMODE = O).....	49

3.16.2.6 New Greetings Mode with reactivation option to OpenScape Xpressions Mode (UCMODE = N).....	50
3.16.2.7 OpenScape Xpressions WebAssistant Mode only (UCMODE = X).....	53
3.16.2.8 Unauthorized Mode - Voice mail tab disabled (UCMODE = D).....	53
3.16.3 Basic Instructions to use the New Voicemail settings.....	54
3.16.3.1 New Interface of Voice Mail Settings.....	54
3.16.3.2 How to Record and Play on Phone.....	55
3.16.3.3 How to Upload and Download Greetings.....	59
3.16.3.4 How to Do not allow recording of voice mails.....	61
3.16.3.5 How to Set Automatic Call Forward to Voice mail (only for Vacation greeting).....	62
3.16.3.6 How to Set Business Greeting Time Profiles (only for Business greetings).....	64
3.16.4 Restrictions of the New UC greetings mode.....	65
3.17 List of Useful Contacts.....	66
3.18 Active Conference Notification.....	68
3.19 Active Conference Tab and Avatars.....	69
3.20 How to allow Softphones to automatically answer conference calls.....	69
3.21 How to configure the Headset Service.....	69
3.22 How to configure the Password Reset Service.....	69
3.23 How to configure the Password Expiration Notification Service.....	71
3.24 How to enable the Whiteboard feature.....	72
3.25 How to enable the Survey feature.....	72
3.26 How to enable the Chat in Conference feature for UC users.....	73
3.27 How to enable the Chat in Conference feature for guest users.....	73
3.28 How to enable audio sharing during screen share.....	74
3.29 How to enable the Hands Up feature.....	74
3.30 How to enable the My Notes feature.....	75
3.31 How to enable the integration between multiple features.....	75
3.32 How to enable the OpenScape Add-ins download option.....	76
3.33 How to enable the OpenScape Headset integration download option.....	76
3.34 How to enable the Video Effects feature.....	77
3.35 How to enable the Call Quality feature.....	78
3.36 How to enable the new Call Forwarding for internal/external call originators feature.....	79
4 System Configuration.....	80
4.1 Configuration Requirements.....	80
4.2 Overview of the Configuration Process.....	87
4.3 Configuration Checklist.....	88
4.4 Changing the Deployment Scenario.....	94
4.4.1 Changing from Integrated Deployment to Small Deployment	94
4.4.2 Changing from Small Deployment to Large Deployment	94
4.4.2.1 Configuring additional OpenScape Media Servers	95
4.4.2.2 Configuring additional Front-End Servers	95
4.4.3 Extending Large Deployment	95
4.4.3.1 Configuring additional OpenScape Media Servers	95
4.4.3.2 Configuring additional Front-End Servers	96
4.5 Configuration Preparations.....	96
4.5.1 Sharing Protocol Ports in Firewall.....	96
4.5.2 Starting OpenScape UC Application.....	96
4.6 General Configuration.....	97
4.6.1 Configuring the Load Balancer for Front-End Computers.....	98
4.6.2 Configuring the Load Balancer for Facade Servers.....	102
4.6.3 Configuring IPsec.....	103
4.6.4 Activating Licenses.....	103
4.6.5 Configuring the Number of Connections for OpenScape Web Client.....	104
4.6.6 Configuring settings for the OpenScape Web Client in the Internet Explorer.....	105
4.6.7 Configure the contact display merging.....	105

4.6.8 Configuring the Presence Service.....	107
4.6.9 Creating a User Profile.....	109
4.7 Configuring the Communications System Connection.....	111
4.7.1 Connecting OpenScape Voice.....	111
4.7.1.1 Checking OpenScape Voice Dependencies.....	112
4.7.1.2 Configuring a reduced OpenScape Voice Assistant.....	119
4.7.1.3 Configuring the OpenScape Voice System in the OpenScape Voice Assistant.....	119
4.7.1.4 Configuring Backup Routing feature for UC calls.....	120
4.7.1.5 Configuring the Synchronization of Business Group Data.....	121
4.7.1.6 Configuring the SIP Trunk in OpenScape Voice.....	122
4.7.1.7 Configuring the CSTA Link to OpenScape Voice.....	125
4.7.1.8 Configuring the Number of CSTA Sessions in OpenScape Voice.....	126
4.7.1.9 Configuring Office Codes.....	127
4.7.1.10 Configuring Prefixes.....	128
4.7.1.11 Configuring Packet Filters for Media Server Computer Systems.....	129
4.7.1.12 Enabling Call Forwarding for Internal and External Originators for OpenScape Voice Subscribers.....	132
4.7.2 Connecting an OpenScape 4000 System.....	133
4.7.2.1 Configuring the SIP Trunk in OpenScape 4000.....	134
4.7.2.2 Activating the Import / Export-API in OpenScape 4000 Assistant.....	134
4.7.2.3 Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager.....	134
4.7.2.4 Configuring a CSTA Connection to an individual OpenScape 4000 System.....	136
4.7.2.5 Enabling Call Forwarding for Internal and External Originators for OpenScape 4000 Subscribers.....	137
4.7.3 Connecting various Communications Systems simultaneously (mixed Scenario).....	137
4.7.3.1 Configuring the Trunk between OpenScape Voice and OpenScape 4000.....	138
4.7.3.2 Configuring the OpenScape Voice Connection.....	138
4.7.3.3 Configuring the Connection to OpenScape 4000.....	139
4.7.4 Configuring Address Translation Contexts.....	140
4.7.5 Address Translation – Configuring St. Routing.....	142
4.7.6 Configuring the SIP Trunk in the OpenScape Media Server.....	144
4.7.7 Creating User Accounts.....	147
4.8 Configuring the One-number Service (ONS).....	151
4.8.1 Configuring the ONS Number.....	151
4.8.2 Activating the One-Number Service in OpenScape Voice.....	153
4.8.3 Configuring the CTI Monitoring in OpenScape Voice.....	154
4.8.4 Configuring an alternative Destination in OpenScape Voice.....	155
4.8.5 Configuring Device Settings.....	155
4.8.5.1 OptiPoint Devices and OpenScape Desktop Client.....	155
4.8.5.2 OpenStage Device.....	155
4.9 Configuring the Conference Portal.....	156
4.9.1 Configuring the Conference Portal Acces.....	156
4.9.2 Configuring a CTI Connection.....	158
4.9.3 Configuring the Conference Component.....	159
4.9.4 Configuring the Phone Number Normalization.....	161
4.9.5 Activating RTCP for Video Conferences.....	162
4.9.6 Configuring the Conference Portal for Media Server Farm.....	163
4.9.7 Configuring the Conference Portal for Integrated Deployment with External Media Server for Video Conferences.....	170
4.9.8 Configuring the SMTP Server Connection.....	179
4.9.9 Configuring Video Systems.....	180
4.9.9.1 Counterpath Bria.....	180
4.9.9.2 Eyebeam.....	181
4.9.9.3 Siemens VHD 100 / 400 (LifeSize Express / Team).....	181
4.9.9.4 Polycom HDX 4500.....	181

4.9.9.5 Polycom HDX 6000.....	181
4.9.9.6 Polycom HDX 7000.....	181
4.9.9.7 Polycom VVX 1500.....	182
4.9.9.8 Tandberg E 20.....	182
4.9.9.9 OpenScape Fusion.....	182
4.10 Configuring the Voice Portal.....	182
4.10.1 Configuring the User Access to the Voice Portal.....	183
4.10.2 Configuring the Guest Access to the Voice Portal.....	184
4.10.3 Configuring a Voicemail Number for Users.....	186
4.10.4 Configuring the Phone Number Normalization.....	187
4.10.5 Configuring the Voice Portal for Media Server Farm.....	189
4.10.6 Configuring the Replication of Voice Portal Greetings.....	192
4.11 Connecting Microsoft Exchange.....	193
4.11.1 Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019.....	193
4.11.1.1 Configuring a technical User Account for Microsoft Exchange 2013 / 2016 / 2019.....	194
4.11.1.2 Configuring the Receive Connector for Microsoft Exchange 2013/ 2016 / 2019.....	195
4.11.1.3 Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019.....	198
4.11.1.4 Configuring the Groupware-Exchange Connector for Microsoft Exchange 2013 / 2016 / 2019...	199
4.11.1.5 Creating User Assignments for Microsoft Exchange 2013/ 2016 / 2019.....	204
4.11.1.6 Importing User Assignments for Microsoft Exchange 2013/ 2016 / 2019.....	209
4.11.1.7 Configuring Access to Microsoft Outlook Contacts for Microsoft Exchange 2013/ 2016 / 2019...	210
4.11.1.8 Configuring restricted Access to private Microsoft Exchange 2013/ 2016 / 2019 Contacts.....	211
4.12 Connecting Microsoft Exchange Online.....	211
4.12.1 Configuring the Connection to Microsoft Exchange Online.....	211
4.12.1.1 Enabling the Multiline connector for Microsoft Exchange Online.....	211
4.12.1.2 Exporting Certificates for the AzureAD Configuration (oAuth).....	212
4.12.2 Configuring Microsoft Exchange Online.....	214
4.12.2.1 For previous version of Microsoft Azure Portal.....	214
4.12.2.2 For new version of Microsoft Azure Portal.....	215
4.12.3 Configuring the OpenScape UC Application for the Connection with Microsoft Exchange Online.....	217
4.12.4 Configuring an app in Azure AD for OpenScape UC Clients access to OL Local Contacts and Out of Office notification.....	220
4.13 Synchronizing the MS Teams Presence with Openscape UC.....	221
4.13.1 Configuration in MS Azure Active Directory.....	222
4.13.2 UC MS Graph Connector app in Facade node.....	223
4.13.3 Configuration of the callback uri in the HApoxxy.....	224
4.13.4 Configuration of UC Teams Graph Connector in UC BE.....	224
4.13.5 Startup and logs on the façade node.....	225
4.13.6 User provisioning.....	225
4.13.7 Administration of technical users and application secrets.....	225
4.14 Configuring the IBM Lotus Domino Connection.....	226
4.14.1 Creating a Linux User and Linux Group.....	226
4.14.2 Configuring the Connector Server.....	227
4.14.3 Stopping the Connector Server.....	229
4.14.4 Creating a technical User Account.....	230
4.14.5 Configuring Access Privileges for Mailboxes.....	230
4.14.6 Configuring Access Privileges for Files.....	231
4.14.7 Configuring the Groupware-Domino Connector.....	231
4.14.8 Configuring the IBM Lotus Notes System Configuration.....	232
4.14.9 Creating User Assignments.....	233
4.14.10 Importing User Assignments.....	238
4.14.11 Configuring Access to IBM Lotus Notes Contacts.....	239
4.14.12 Configuring the IBM Lotus Domino Server for OpenScape Conference Extension.....	239
4.14.12.1 Dividing a multilingual Mail Template.....	241
4.14.12.2 Preparing the Configuration.....	242
4.14.12.3 Copying Images into the Mail Template Database.....	242

4.14.12.4 Copying Script Libraries into the Mail Template Database.....	243
4.14.12.5 Copying Form Actions into the Mail Template Database.....	245
4.14.12.6 Changing the Forms' Code.....	247
4.14.12.7 Creating a Configuration Button for Conferences.....	249
4.14.12.8 Configuring the Activation of the Presence Plugin Thread.....	251
4.14.12.9 Additional Adaptation of the templates for Notes.....	251
4.14.12.10 Configuring the Deletion of Conferences.....	254
4.14.12.11 Activating the Configuration for IBM Lotus Notes Users.....	257
4.15 Configuring the LDAP Directory Connection.....	260
4.15.1 Configuring the Connection to the LDAP Directory.....	261
4.15.2 UC LDAPs connection configuration.....	263
4.15.3 Restarting the LDAP Connector Service.....	264
4.15.4 Configuring the LDAP User Access.....	265
4.15.5 Rebooting the Facade Server.....	266
4.16 Configuring the Instant-Messaging Connection.....	266
4.16.1 Configuring the Openfire Server.....	267
4.16.2 Creating Packet Filter Rules in OpenScape Voice.....	269
4.16.3 Configuring the IM Address for OpenScape Users.....	270
4.16.4 Activating IM Communication Archiving.....	271
4.16.5 Creating and synchronizing Openfire User Accounts.....	272
4.16.6 Disabling IM Communication Archiving.....	273
4.16.7 Delete Chat Message.....	273
4.17 Configuring the Connection to OpenScape Xpressions.....	273
4.17.1 Planning Details for an m × n Connection.....	274
4.17.2 Configuring Voicemail Numbers for Users.....	276
4.17.3 Assigning the Access Privilege.....	278
4.17.4 Displaying PhoneMail Settings.....	279
4.17.5 Configuring XPR PhoneMail.....	279
4.17.6 Configuring the Voice Portal Access.....	281
4.17.7 Installing the XPR Import Script.....	285
4.17.8 Configuring the XPR Import Script.....	286
4.17.9 Creating an XPR Import File.....	286
4.17.10 Importing an XPR Import File.....	287
4.17.11 Rebooting the XPR Server.....	289
4.17.12 Assigning a Privilege to XPR Users.....	289
4.17.13 Configuring the Web APL of OpenScape Xpressions.....	290
4.17.14 Configuring PhoneMail Script Settings.....	292
4.17.15 Creating a UC Application Import File.....	293
4.17.16 Importing a UC Application Import File.....	293
4.17.17 Configuring OpenScape Web Client.....	294
4.17.18 Changing UC Application User Profiles.....	296
4.17.19 Nuance services to be verified to allow simultaneous availability of WebAssistant and the Voice Mail tab in WebClient.....	297
4.18 Configuring the System Networking	298
4.18.1 Configuring the Openfire Server.....	299
4.18.2 Configuring the Conference Portal.....	302
4.18.3 Configuring the Size of the JVM Heap.....	303
4.19 Configuring Inbound / outbound device.....	303
4.20 Configuring WebRTC functionality.....	304
4.20.1 Prerequisites.....	304
4.20.2 Restrictions.....	305
4.20.3 WebRTC licenses.....	305
4.20.4 Configuring WebRTC in OSV.....	306
4.20.4.1 Configuration of trusted list in OSV.....	306
4.20.4.2 Configuration of trusted subscribers.....	307
4.20.5 Configuring WebRTC with a multiple Media Server system.....	308

4.20.6 Configuring WebRTC in UC.....	308
4.20.6.1 Configuration of certificates in BE server.....	310
4.20.6.2 Importing the certificates and private key to the keystore of the Media Server and Front End servers.....	312
4.20.6.3 JWT token protection.....	314
4.20.7 Configuring WebRTC in OpenScape 4000.....	315
4.20.8 OpenScape Voice Signaling Protocol data synchronization.....	315
4.20.8.1 Singaling Protocol fields are empty.....	316
4.20.9 Extending the setup to internet usage.....	316
4.20.9.1 Configuring TURN server from Media Server.....	316
4.20.9.2 Disabling ICMP error counting and Bandwidth adaptation within the streaming route of the MediaServer.....	318
4.20.9.3 Video Codecs.....	319
4.20.9.4 Configuring the WebRTC Service.....	320
4.20.9.5 Configuring WebRTC for a multiple Media Server system.....	321
4.20.9.6 Configuring HAProxy.....	322
4.20.10 Configuring UC users.....	325
4.20.10.1 Configuring profiles.....	325
4.20.10.2 Configuring devices (OND or ONS).....	326
4.20.11 Configuring WebRTC Guest Access.....	327
4.20.11.1 Restrictions for WebRTC Guest Access.....	327
4.20.12 Configuring QoS.....	330
4.20.13 Configure WebRTC Screen Sharing.....	332
4.20.13.1 Prerequisites.....	332
4.20.13.2 Configuration.....	332
4.20.14 Hunt Group support in WebRTC softphone.....	333
4.20.15 Configuring WebRTC Video resolution.....	333
4.21 Enabling UC Desktop App download link.....	334
4.22 Installing Keycloak.....	334
5 System Management for overlapping OpenScape Components.....	339
6 System management for the components of OpenScape UC Application.....	340
6.1 Dashboard for the System Nodes of OpenScape UC Application.....	340
6.2 UC User Administration.....	341
6.2.1 How to Add a UC User Account.....	344
6.2.2 How to Edit a UC User Account's Settings.....	346
6.2.3 How to Delete a UC User Account.....	348
6.2.4 How to Display Bound Licenses of a UC User.....	348
6.2.5 How to Configure Existing Voicemail Numbers for a UC User Account.....	349
6.2.6 How to Configure Existing Voicemail Numbers for a UC User Account.....	349
6.2.7 How to Configure a New Voicemail Number for a UC User Account.....	350
6.2.8 How to Configure Subscriber Phone Number(s) for a UC User Account.....	350
6.2.9 How to Delete a Subscriber Phone Number(s) from a UC User Account.....	352
6.2.10 How to Configure UC User's External Identifiers.....	353
6.2.11 How to Configure UC User Visibility Groups.....	354
6.3 Team Configuration Overview.....	354
6.3.1 How to Display Unified Communication Teams.....	355
6.3.2 How to Add/Edit UC Teams.....	356
6.3.3 How to Delete a UC Team.....	358
6.3.4 How to Add a UC Team Member.....	359
6.3.5 How to Delete a UC User from a Team.....	360
6.3.6 How to Display Names in Journals of Team Members.....	362
6.3.7 How to modify the Team Toaster delay pop up notification.....	362
6.4 Visibility Groups Configuration Overview.....	363
6.4.1 How to Add/Edit a Visibility Group.....	363

6.4.2 How to Delete a UC Visibility Group.....	364
6.4.3 How to Assign Visibility Groups Feature to an Administrator.....	364
6.5 Contact List Management.....	365
6.5.1 How to Display list of Global Contact.....	366
6.5.2 How to Add a Global Contact.....	367
6.5.3 How to Edit a Global Contact.....	368
6.5.4 How to Link a Global Contact to a UC User.....	369
6.5.5 How to Link a Global Contact to a UC User.....	369
6.5.6 How to Define the Global Contact List as Active Contact List.....	370
6.5.7 How to Cancel the Status of an Active Global Contact List.....	370
6.5.8 How to Specify a Storage Location for Private Contact Lists.....	371
6.6 Communication System Resources.....	371
6.6.1 How to Display Office Codes.....	373
6.6.2 How to Edit Office Codes.....	374
6.6.3 How to Display Prefixes.....	375
6.6.4 How to Edit Prefixes.....	376
6.6.5 How to Display Voice Subscribers.....	377
6.6.6 How to Edit Voice Subscribers.....	378
6.6.7 How to Display Media Server Office Codes.....	380
6.6.8 How to Display Media Server Office Codes.....	380
6.6.9 How to Add Media Server Office Code.....	381
6.6.10 How to Delete Media Server Office Codes.....	382
6.6.11 How to Add Media Server Prefixes.....	382
6.6.12 How to Display Media Server Prefixes.....	383
6.6.13 How to Delete Media Server Prefixes.....	384
6.6.14 How to Display Media Server Conference Devices.....	384
6.6.15 How to Add Media Server Conference Device.....	385
6.6.16 How to Delete Media Server Conference Device.....	386
6.7 Address Translation Context Overview.....	386
6.7.1 How to Add Address Translation Context.....	387
6.7.2 How to Display Address Translation Contexts.....	389
6.7.3 How to Edit Address Translation Context.....	390
6.7.4 How to Add an Address Translation Station Routing.....	392
6.7.5 How to Display Address Translation Station Routing.....	393
6.8 HiPath OpenScape Configuration.....	393
6.8.1 How to Display OpenScape Voice switch Connections.....	394
6.8.2 How to Add an OpenScape Voice Connection.....	394
6.8.3 How to Display Media Server Connections.....	396
6.8.4 How to Add a Media Server Connection.....	396
6.9 LDAP Connection.....	397
6.9.1 How to Display Settings for LDAP Connection.....	401
6.9.2 How to Add an LDAP Directory Connection.....	401
6.9.3 How to Edit an LDAP Directory Connection.....	410
6.9.4 How to Clone an LDAP Directory Connection.....	412
6.9.5 How to Delete an LDAP Directory Connection.....	412
6.9.6 Using avatar pictures in a UC system on a LDAP Directory Connection.....	413
6.10 UC Rapidstat Overview.....	413
6.10.1 UC Rapidstat Report in HTML.....	414
6.10.2 UC Rapidstat Report Text file.....	418
6.10.3 How to Display UC Rapidstat.....	420
6.10.4 How to Configure UC Rapidstat Settings.....	421
6.10.5 How to Configure manually the partition specific settings for UC Rapidstat xml files.....	423
6.11 Managing Groupware Services.....	425
6.11.1 Groupware Service Concept.....	425
6.11.2 Adding a Groupware Connection.....	427
6.11.3 Displaying a Groupware Connection.....	428

6.11.4 Displaying / Editing Groupware-Domino Connector Settings.....	428
6.11.5 Displaying / Editing the IBM Lotus Notes System Configuration.....	429
6.11.6 Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services.....	431
6.11.7 Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP.....	433
6.11.8 Configuring the encrypted Transmission between Groupware-Exchange Connector and Microsoft Exchange Servers.....	435
6.11.8.1 Loading Certificates from the Microsoft Exchange Servers.....	435
6.11.8.2 Importing Certificates in OpenScope UC Application.....	437
6.11.8.3 Activating the Encryption.....	438
6.11.9 Displaying / Editing Settings for an independent SMTP Server Connection.....	439
6.11.10 Configuring the Contact Data Replication of the Groupware Service.....	440
6.11.11 Configuring restricted Access to private Groupware Contacts.....	443
6.11.12 Handling Groupware Exchange Contact Pictures.....	444
6.12 Managing Instant-Messaging Connections.....	445
6.12.1 Concept of the Instant Messaging Connection.....	445
6.12.2 Displaying / Editing Instant-Messaging Connections.....	445
6.13 Backing up and restoring general OpenScope System Components.....	448
6.13.1 General Memory Requirements for backing up Data of the Application Computer.....	448
6.13.2 Backing up a File System for a Deployment Scenario different from Integrated Deployment manually.....	449
6.13.3 Restoring OpenScope Configuration Data.....	452
6.13.4 Restoring the OpenScope System for Integrated Deployment.....	454
6.13.5 Restoring UC Application for a Deployment Scenario different from Integrated Deployment.....	457
6.13.6 Restoring OpenScope Voice for a Deployment Scenario different from Integrated Deployment.....	460
6.13.7 Restoring the Response File from a Backup Set.....	460
6.14 Managing the Voice Portal.....	462
6.14.1 Creating an individual User Access.....	462
6.14.2 Creating an individual Guest Access.....	464
6.14.3 Configuring the Default Language of a Voice Portal Access.....	465
6.14.4 Changing the Phone Number Use by the Voice Portal in Case of Forwardings.....	466
6.15 Managing the Conference Portal.....	467
6.15.1 Configuring Security Settings for outgoing Conference Connections.....	468
6.15.2 Configuring the Default Language for outgoing Conference Connections.....	469
6.15.3 Configuring the Conference Portal Access for another existing Language.....	469
6.15.4 Changing Music-on-Hold for the Conference Portal.....	470
6.15.5 Restricting Media Types and Locations for Conference Services.....	471
6.15.6 Configuring the maximum Number of Conference Participants.....	472
6.15.7 Changing the E-Mail Notification Text for Conferences.....	473
6.15.8 Changing the Participant Signaling Restriction.....	475
6.15.9 Disabling the Full HD Resolution.....	476
6.15.10 Configuring Video Layouts used.....	476
6.15.10.1 Common Video View Layout.....	477
6.15.11 Configuring Mailbox Recognition of the Conference Portal.....	478
6.15.12 Managing Video Layouts for Conferences.....	479
6.15.13 Managing Conferences independently of OpenScope UC Application.....	479
6.16 Managing the OpenScope Media Server.....	479
6.17 Managing OpenScope Web Client (Webserver Components).....	479
6.17.1 Changing the HTTP / HTTPS Port for OpenScope Web Client.....	480
6.17.2 Enabling the Display of non UC Users Name in Call Control and Journal.....	481
6.17.3 Enabling special keys used by WebClient regarding incoming calls.....	482
6.17.4 Enabling the Location Fields in the Web Client.....	482
6.17.5 Enabling the Download of the OpenScope Desktop Integration Tool.....	483
6.17.6 Specifying the Synchronization Strategy for Contact Details.....	484
6.17.7 Scheduling the Synchronization of Private Contact Details.....	484
6.17.8 WebClient UI Customization.....	493
6.17.9 Browsers and Language.....	493

6.17.10 Import of contact data from other sources.....	493
6.17.11 Configuration for Team : Team shall take my calls.....	494
6.17.12 Browsers and Web Sockets.....	495
6.17.13 Enabling the Set all read button in Call History.....	495
6.17.14 Limit the entries in UC Journal / Call History.....	495
6.17.15 Reduced Set of presence states.....	496
6.17.16 Enable Voicemail tab for Settings.....	496
6.17.17 Reducing size of recorded audio files.....	497
6.17.18 Handling Profile Rules.....	498
6.17.19 Display the second e-mail (home e-mail).....	498
6.17.20 Hide the WebRTC Guest Access button in UC Conferences.....	499
6.17.21 Changing the Authentication Cookie Management Policy.....	499
6.17.22 Configuration for SIP DNS SRV.....	500
6.17.23 Display the Emergency Call Disclaimer.....	500
6.17.24 Modification of Content-Security-Policy.....	501
6.18 Managing the Facade Server.....	501
6.18.1 Concept of the Facade Server Management.....	501
6.18.2 Configuring the Facade Server.....	504
6.18.3 Activating SSL for Facade Servers.....	505
6.19 Managing the Openfire Server.....	505
6.19.1 Resynchronization of the Presence Access Privileges in a networked UC Application Environment with several Openfire Servers.....	505
6.19.2 Changing the Openfire Server Certificates.....	505
6.19.3 Searching archived Connection Data.....	508
6.20 Managing the E-Mail Service.....	509
6.20.1 Concept of the E-Mail Service.....	509
6.20.2 Configuring Send Settings for Notification E-mails.....	511
6.20.3 Configuring Settings for Conference Notification.....	512
6.20.4 Configuring a Callback from a Notification.....	513
6.21 Configuring SSO (Single Sign-On).....	514
6.21.1 Single Sign-on Concept.....	514
6.21.2 Configuring the Server for Single Sign-On of the non-SOAP-based Clients.....	517
6.21.2.1 Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems.....	518
6.21.2.2 Configuring a technical User Account.....	518
6.21.2.3 Creating the KEYTAB File.....	519
6.21.2.4 Configuring JAAS.....	523
6.21.2.5 Creating User Assignments.....	527
6.21.2.6 Importing User Assignments.....	530
6.21.2.7 Restarting OpenScape UC Application.....	530
6.21.3 Configuring the Server for Single Sign-On of the SOAP-based Clients.....	531
6.21.3.1 Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems.....	531
6.21.3.2 Configuring a technical User Account.....	532
6.21.3.3 Creating the KEYTAB File.....	533
6.21.3.4 Configuring the SPNEGO-IAE Service.....	537
6.21.3.5 Changing the Buffer Sizes.....	538
6.21.3.6 Configuring JAAS_IBM.....	539
6.21.3.7 Creating and importing User Assignments.....	540
6.21.3.8 Restarting OpenScape UC Application.....	541
6.21.4 Deleting Windows Login Information.....	541
6.21.5 Configuring a Browser for Single Sign-On.....	541
6.21.5.1 Internet Explorer Settings.....	542
6.21.5.2 Firefox Settings.....	542
6.21.6 Configuring UC Application Clients for Single Sign-On.....	543
6.21.7 Setting up SSO with Windows AD.....	543
6.21.7.1 SPNEGO IAE and/or WebClient Configuration File: /opt/siemens/common/conf/krb5.conf.....	544
6.21.7.2 WebClient only Configuration.....	544

6.21.7.3 SPNEGO IAE only Configuration.....	545
6.21.8 Support of Single Sign On (SSO) for multiple Domains.....	545
6.22 Configuring the Use of Windows Login Data.....	547
6.22.1 Concept of Using Windows Login Data.....	547
6.22.2 Configuring the Use of Windows Login Data without simultaneous Use of SSO for OpenScape Web Client.....	548
6.22.2.1 Activating the Windows Authentication.....	548
6.22.2.2 Changing the Kerberos Configuration File.....	548
6.22.2.3 Creating User Assignments.....	550
6.22.2.4 Importing User Assignments.....	552
6.22.2.5 Restarting OpenScape UC Application.....	552
6.22.3 Configuring the Use of Windows Login Data with simultaneous Use of SSO for OpenScape Web Client.....	553
6.22.3.1 Activating the Windows Authentication.....	553
6.22.3.2 Determining Configuration Files used.....	554
6.22.3.3 Creating User Assignments.....	555
6.22.3.4 Importing User Assignments.....	558
6.22.3.5 Restarting OpenScape UC Application.....	558
6.23 Controlling Busy Signaling (Busy-on-Busy).....	559
6.23.1 Busy Signaling (Busy-on-Busy) Concept.....	559
6.23.2 Activating Busy-on-Busy.....	559
6.23.3 Busy on Busy for ONS incoming call.....	560
6.23.4 Busy on Busy for Microsoft Teams Presence.....	563
6.24 Executing Application Operations for OpenScape UC Application.....	563
6.25 Further administrative Tasks.....	564
6.25.1 Configuring a reduced OpenScape Voice Assistant.....	565
6.25.2 Starting/restarting OpenScape UC Application.....	567
6.25.2.1 Rebooting the UC Application Services of a Computer System.....	568
6.25.2.2 Rebooting UC Application Services of all Computer Systems.....	568
6.25.3 Saving the Security Certificate for the CMP.....	569
6.25.4 Checking the Availability of CSTA Connections.....	569
6.25.5 Checking the CSTA Connection Function.....	571
6.25.6 Changing the User Passwords Policies.....	572
6.25.7 Changing Policies for User PINs.....	576
6.25.8 Synchronizing License Assignments anew.....	580
6.25.9 Creating a Firewall Rule in OpenScape Voice.....	581
6.25.10 Changing IP Addresses / FQDNs of the UC Application Computer Systems.....	582
6.25.10.1 Changing the IP Address / FQDN for Small Deployment.....	583
6.25.10.2 Changing IP Addresses / FQDNs for a Deployment Scenario different from Small Deployment.....	584
6.25.10.3 Creating both IPV4 and IPV6 compatible Servers.....	587
6.25.11 Configuring the IPV6 Support for OpenScape Media Server.....	587
6.25.12 Configuring the HTTPS Port for CMP Access.....	587
6.25.13 Activating HTTP Port for Framework.....	588
6.25.14 Activating the anonymized Originator Address for automatic e-mails.....	589
6.25.15 Configuring Scheduled Message Routing.....	590
6.25.16 Transmitting Information about OpenScape 4000 Resources to OpenScape UC Application.....	591
6.25.17 Activating the Call Acceptance for remote preferred Devices.....	592
6.25.18 Managing Network Address (NAT) Translations.....	592
6.25.18.1 Structure of an NAT Mapping Table.....	593
6.25.18.2 Configuring Network Address (NAT) Translations.....	594
6.25.19 Suppressing Features for managing preferred Devices in the Clients.....	597
6.25.20 Starting all Conferences as Video Conference.....	598
6.25.21 Copying an OpenScape Voice Resource with changed Subscriber Type.....	599
6.25.22 Configuring the Status Monitoring for OpenScape Voice Multiline Hunt Groups (MLHG).....	601
6.25.23 Restricting the Visibility of Contacts based on Groups.....	602

6.25.24 Changing the Service Account for UC Application Services.....	603
6.26 Managing OpenScape Outlook Extensions.....	604
6.27 Configuring WebRTC support to OSV failover.....	604
6.27.1 DNS SRV Configuration.....	605
6.27.2 UC-OSV Configuration.....	606
6.28 OSMO Configuration via QR Code.....	607
7 System Monitoring.....	608
7.1 Logging OpenScape UC Application.....	608
7.1.1 Checking the System Components' Start.....	608
7.1.2 Activating the Conferencing Component Logging.....	611
7.1.3 Activating the Domain Component Logging.....	613
7.1.4 Collecting Log and Dump Information automatically.....	614
7.1.4.1 The collect.sh Script	615
7.1.4.2 logfiles-<...>.tar file.....	615
7.1.4.3 dumpfiles-<...>.tar file.....	615
7.1.4.4 Starting the Collection of Log and Dump Information.....	616
7.1.5 Putting out Software Versions of the UC Application Components (productInventory.sh).....	617
7.2 Logging OpenScape Voice.....	617
7.3 Logging the SIP Traffic between OpenScape Voice and a Device.....	617
7.4 Logging OpenScape 4000.....	618
7.5 Logging the Groupware Service.....	618
7.5.1 Log Files.....	619
7.5.2 Logging Configuration.....	619
7.6 Logging the Web Server Component.....	622
7.6.1 Concept of the Web Server Component Logging.....	623
7.6.2 Determining Additional Data for Logging.....	624
7.6.3 Reproducing a Problem Using the Web Server Component.....	626
7.6.4 Logging the OpenScape Desktop Integration Tool.....	627
7.6.4.1 Concept of the OpenScape Desktop Integration Tool Logging.....	628
7.6.4.2 Activating the Logging for OpenScape Desktop Integration Tool across the System.....	629
7.6.4.3 Activating the Logging for OpenScape Desktop Integration Tool specific to Clients.....	629
7.7 Logging Nuance Vocalizer (TTS).....	630
7.8 Compression of Log-files for WebClient.....	630
8 Statistics Data.....	631
8.1 Raw Statistics Output of the Conference Portal.....	631
8.1.1 Statistics Concept of the Conference Portal.....	631
8.1.2 Structure of the Conference Portal Statistics Data.....	632
8.1.2.1 Statistics Messages for the Event ConferenceStartedEvent.....	635
8.1.2.2 Statistics Messages for the Event ConferenceStoppedEvent.....	638
8.1.2.3 Statistics Messages for the Event ConferenceProlongedEvent.....	638
8.1.2.4 Statistics Messages for the Event VoiceConferenceAddedEvent.....	639
8.1.2.5 Statistics Messages for the Event VideoConferenceAddedEvent.....	639
8.1.2.6 Statistics Messages for the Event WebConferenceAddedEvent.....	640
8.1.2.7 Statistics Messages for the Event UserState_Joined.....	640
8.1.2.8 Statistics Messages for the Event UserState_Left.....	641
8.1.2.9 Statistics Messages for the Event UserState_Rejected.....	641
8.1.2.10 Statistics Messages for the Event userconnectingfailedEvent.....	642
8.1.2.11 Statistics Messages for the Event UserAddedEvent.....	642
8.1.3 Activating the Raw Statistics Output for the Conference Portal.....	643
8.1.4 Configuring the Output Settings for the Conference Portal Raw Statistics.....	643
8.2 Raw Statistics Output of the OpenScape Media Server.....	644
9 Upgrading external Systems.....	645
9.1 Upgrading HiPath 4000 V6 to OpenScape 4000 V7.....	645

10 Configuring a Certificate Strategy.....	646
10.1 Dependencies as regards the OpenScope Deployment Scenario.....	646
10.2 Contemplated Customer Environments.....	652
10.2.1 Customer Environment 1 (CE 1) – PKI with CA	652
10.2.2 Customer Environment 2 (CE 2) – PKI with CA and CSR	653
10.2.3 Customer Environment 3 (CE 3) – PKI without CA	653
10.2.4 Customer Environment 4 (CE 4) – PKI planned	653
10.3 Overview of the Configuration Steps.....	653
10.4 Preparing the Configuration of the Certificate Strategy.....	655
10.4.1 Determining the OpenScope Setup Directory.....	656
10.4.2 Determining the Keytool Command.....	656
10.4.3 Determining the Keystore Directory.....	657
10.4.4 Determining the Directory for the SSL / TLS Configuration.....	658
10.4.5 Defining an X.500 Distinguished Name.....	658
10.5 Configuring a simple Certificate Authority.....	661
10.5.1 Preparing the Certificate Authority.....	661
10.5.2 Creating self-signed Root Certificates.....	663
10.6 Creating a Pair of Keys for the Application Computer.....	665
10.7 Creating Certificate Sign Requests for the Application Computer.....	666
10.8 Creating a Pair of Keys for the Frontend Computer.....	667
10.9 Creating a Certificate Sign Request for the Frontend Computer.....	668
10.10 Creating a Pair of Keys for the Facade Server.....	669
10.11 Creating a Certificate Sign Request for the Facade Server.....	671
10.12 Signing Certificate Sign Requests.....	672
10.13 Importing a Certificate in the Server Keystore.....	673
10.14 Storing a provided PKCS#12 File.....	676
10.15 Activating a Server Keystore for the CMP.....	677
10.16 Configuring a Server Keystore for the Application Computer.....	677
10.17 Configuring Certificate and Keys for the BCom Component.....	678
10.18 Configuring a Server Keystore for the Multi-Node System.....	679
10.19 Configuring a Server Keystore for the Facade Server.....	681
10.20 Importing the Root Certificate in the Client Browsers.....	682
10.20.1 Displaying the Root Certificate.....	683
10.20.2 Checking the Root Certificate.....	684
10.20.3 Installing the Root Certificate.....	684
10.21 Importing the Root Certificate in the Mobile Phones.....	685
10.22 Configuring the Certificate for the SPML Interface.....	685
10.23 Configuring the Certificate for the UC Graph Connector.....	687
10.24 Supplementing Instructions.....	687
10.24.1 Creating a secure Password.....	687
10.24.2 Combining Certificate Files to a Certificate Chain.....	688
10.24.3 Converting the Format of a Certificate Chain from DER into PEM.....	689
10.24.4 Converting the Format of a Certificate Chain from PKCS#12 into PEM.....	689
11 IPsec Configuration.....	691
11.1 Using IPsec.....	691
11.2 Configuring IPsec for CSTA Connections.....	692
11.2.1 Configuring OpenScope Voice for IPsec-based CSTA Connections.....	692
11.2.2 Configuring OpenScope UC Application for IPsec-based CSTA Connections.....	695
11.3 Configuring IPsec for MGCP Connections.....	699
11.3.1 Configuration for Small Deployment.....	699
11.3.1.1 Configuring OpenScope Voice for IPsec-based MGCP Connections (Small Deployment).....	700
11.3.1.2 Configuring OpenScope UC Application for IPsec-based MGCP Connections (Small Deployment).....	701
11.3.2 Configuration for Large Deployment.....	705
11.3.2.1 Configuring OpenScope Voice for IPsec-based MGCP Connections (Large Deployment).....	706

11.3.2.2 Configuring OpenScape UC Application for IPsec-based MGCP Connections (Large Deployment).....	708
11.4 Operating System Upgrade SLES 12 SP5 or SLES 15 SP5.....	712
11.4.1 Changing the Endpoint Configuration of OpenScape Voice.....	712
11.4.2 Changing the IPsec Configuration of OpenScape UC Application.....	713
12 Data Structure of the Domain Management Data.....	714
12.1 Overview of the Domain Management Data.....	714
12.2 Accessing the Domain Management Data of a UC Application System.....	714
12.3 Basic Structure of a CSV File.....	714
12.4 Editing CSV Files manually.....	715
12.5 Importing reserved Characters.....	716
12.6 Processing a CSV File while it is being imported.....	716
12.7 Structure of the Domain Management Data.....	718
13 User Privileges for OpenScape UC Application.....	719
14 Voice Portal Settings in the CMP (Voice Portal Plug-in)	728
14.1 Function of the Voice Portal Plug-in.....	728
14.2 Opening the Voice Portal Plug-in.....	728
14.3 Configuring Application Profiles	729
14.3.1 Profile Settings for Profile Type Voice Portal Access.....	730
14.3.2 Profile Settings for Profile Type Guest Portal Access.....	730
14.4 General Application Profile Settings.....	730
14.5 Mailbox Settings of Application Profiles.....	733
14.6 Special Language Settings of Application Profiles.....	734
14.7 Call Settings of Application Profiles.....	734
14.8 Operation Mode Settings of Application Profiles.....	735
15 Conference Portal Settings in the CMP (Conference Portal Plug-in).....	737
15.1 Function of the Conference Portal Plug-in.....	737
15.2 Conference Management	737
15.2.1 Conference settings.....	740
15.2.2 DTMF settings.....	740
15.2.3 DTMF Video.....	742
15.2.4 Timer settings.....	743
15.3 Number configuration.....	745
15.3.1 Bridge numbers	746
15.3.2 Trunk numbers.....	746
15.3.3 Language dependent bridge numbers.....	747
15.4 Configuration.....	747
15.4.1 Bridge Numbers – Media Server Node Configuration.....	747
15.4.2 Bridge Numbers – Media Server Selection.....	748
15.4.3 Miscellaneous Number Settings.....	749
15.5 Media Configuration.....	751
15.5.1 Default language.....	751
15.5.2 Audio Settings.....	751
15.5.3 General - TUI Settings.....	751
15.5.4 Video Settings.....	754
15.5.5 Video Performance Settings.....	755
15.6 Other Settings.....	755
15.6.1 Coman Tool.....	755
15.6.2 Recording.....	756
15.6.2.1 Recording settings.....	757
15.6.2.2 Recording list.....	758
15.6.3 Notification Settings	760
15.6.4 Conference Viewer.....	765

15.6.5 Add join conference beep.....	765
16 General Properties for the Conference Portal.....	766
17 Managing the Conference Video Layout.....	769
17.1 Concept of Managing Video Layouts.....	769
17.2 Structure of the resolution.xml file.....	770
17.3 Structure of the Files screen-layout-...xml.....	770
17.3.1 Structure of the Files screen-layout-accentuated-n+1.xml.....	771
17.3.2 Structure of the Files screen-layout-tiled.xml.....	774
17.3.3 Structure of the Files screen-layout-single.xml.....	774
18 Conference Management Tool Coman.....	775
18.1 Coman Tool Function.....	775
18.2 Import / Export Table for Bulk Processing.....	775
18.3 Processing Conference Scheduling Specifications.....	777
18.4 Logging the Coman Tool for Troubleshooting.....	778
18.5 Installing the Coman Tool.....	778
18.6 Invoking the Coman Tool.....	779
18.7 Invoking the Online Help of the Coman Tool.....	779
18.8 Command Reference for the Coman Tool.....	780
18.8.1 createConferencePerDomainUsers.....	780
18.8.2 deleteAll.....	781
18.8.3 deleteConf.....	782
18.8.4 deleteConfForUser.....	783
18.8.5 exportDomainUsersToXLS.....	784
18.8.6 exportDomainUsersWithPinsToXLS.....	785
18.8.7 exportXLS.....	787
18.8.8 getConfs.....	788
18.8.9 importXLS.....	790
18.8.10 initXLS.....	791
18.8.11 scheduleConf.....	792
18.8.12 startConf.....	793
18.8.13 terminateConf.....	794
19 OpenScape Auto Attendant.....	796
19.1 Function of the OpenScape Auto Attendant.....	796
19.2 Opening the OpenScape Auto Attendant Configuration.....	796
19.3 Configuring Auto Attendant Profiles	797
19.4 General Settings of Auto Attendant Profiles.....	798
19.5 Error Handling Settings of Auto Attendant Profiles.....	800
19.6 Resource Settings of Auto Attendant Profiles.....	801
19.7 Operation Mode Settings of Auto Attendant Profiles	801
19.7.1 Business Hours.....	802
19.7.2 Outside Business Hours.....	803
19.7.3 Weekend.....	804
19.7.4 Public Holidays.....	805
19.7.5 Company Vacation.....	806
19.7.6 Emergency.....	807
19.8 Keypad Layout Settings of the Operation Modes.....	808
19.8.1 Transfer to an Extension	809
19.8.2 Transfer to an Extension (blind Transfer)	810
19.8.3 Hangup	810
19.8.4 Enter an Extension to be transferred to	810
19.8.5 Enter an Extension to be transferred to (blind Transfer)	811
19.8.6 Select a Contact to be transferred to	811
19.8.7 Send a Message to	811

19.8.8 Playback.....	812
19.9 Configuration via Administrator Access.....	812
19.10 Configuring a Routing Workflow.....	813
19.10.1 Creating an Auto Attendant Profile.....	813
19.10.2 Defining general Profile Settings.....	814
19.10.3 Defining Error Handling Settings.....	814
19.10.4 Defining Operation Modes for the Routing Workflow.....	815
19.10.4.1 Defining the Behavior for Business Hours.....	815
19.10.4.2 Defining the Behavior outside Business Hours.....	816
19.10.4.3 Defining the Behavior for Weekends.....	817
19.10.5 Configuring Access to the Routing Workflow.....	818
19.10.6 Configuring Access to the Administrator Access.....	819
19.10.7 Configuring a Routing Workflow for a Media Server Farm.....	820
20 Displaying Directory Numbers in the UC Application Clients.....	821
21 Call Journal / Call History Model of OpenScape Web Client.....	822
21.1 Call History Model for OpenScape Web Client.....	822
21.2 Descriptions in journal / call history entries.....	822
22 Provisioning via LDAP Directories.....	824
23 Adding an External Language in Integrated Simplex.....	825
24 HAProxy Manager Tool.....	826
24.1 Basic Options.....	826
24.1.1 Discard and configure HAProxy.....	827
24.1.2 Discard Facade / Web Client configuration.....	828
24.1.3 Show current configuration.....	828
24.1.4 Restart HAProxy.....	828
24.1.5 About HAProxy.....	828
24.2 Creating certificates without password protection for HAProxy unattended startup.....	828
25 Configuring Internet Access of OpenScape UC clients.....	830
26 Reverse Proxy deployment information.....	831
27 IPV6 Support.....	832
27.1 Prerequisites for installing UC on a IPv6 or IPv4 with IPv6 mixed system.....	832
27.2 Activating IPv6 on a SLES system via yast.....	832
27.3 Configuring knut.response.file.....	833
28 Appendix.....	834
28.1 Overview of the UC Application components that concern the load balancer.....	834
Index.....	836

1 History of Changes

Date	Changes	Reason
03-10-2024	Created V11 Document	
11-9-2025	Removed the following chapters: Enabling Profile Picture Upload in the OpenScape Web Client Disabling First Time User Experience (FTUX) Enabling Conferencing operation in restricted mode	UCBE-38370
21-10-2025	Remove all Web Client 1.0 references	UCBE-38361
29-01-2026	Updated: Single Sign-on Concept on page 514	UCBE-39112

2 About this Manual

This chapter provides information about the following topics:

- [Target Group of this Manual](#)
- [This Manual's Content](#)
- [Manual Structure](#)
- [General Conventions](#)
- [Representation Conventions](#)
- [Specified Deployment Scenarios](#)
- [Specified Default Passwords](#)
- [Acronyms used](#)
- [Continuative Documentation](#)
- [Data Protection and Data Security](#)

2.1 Target Group of this Manual

This manual addresses the following persons:

- Service personnel who configure a communications solution based on OpenScape UC Application.
- Administrators who configure and manage a communications solution based on OpenScape UC Application.

Readers should have the following knowledge to use the information provided in this documentation.

- Knowledge of the general working method of information technology and voice communication systems
- Knowledge of terms used in the information technology and voice communication environment.
- Practical knowledge of how to configure and manage information technology and voice communication systems.
- Practical knowledge of how to administer and configure the Suse Linux operating system.
- Practical knowledge of how to manage the following external systems if an appropriate connection is to be configured with OpenScape UC Application.
 - OpenScape Voice
 - OpenScape 4000
 - Microsoft Exchange Server
 - Microsoft Lync Server
 - IBM Domino Server
 - Openfire Server
 - OpenScape Xpressions Server
 - LDAP directory
- Practical knowledge of how to configure and manage security certificates in Linux if you would like to modify the certificates of the UC Application environment used.

IMPORTANT: Incorrect modifications of the certificates of the UC Application environment may enable unauthorized persons

to access components and data of the system components involved.

2.2 This Manual's Content

This manual describes how to configure a communications solution based on OpenScape UC Application after you have installed all required system components.

Furthermore, this manual tells you:

- How to manage and monitor the communications solution with the CMP.
- How to use the CMP to back up and restore the configuration of the communications solution.

What you do not find in this manual

This manual does not consider the following topics:

- The restrictions that apply for OpenScape UC Application – for example in special system environments. You find information about this in the *OpenScape UC Application, Planning Guide*.
- How to install the described system components on the computer systems. This includes both OpenScape as well as external system components.

You find information about this in the setup manuals of the system components concerned.

- How to install and configure the client components for using the features described here.

You find information about this in the product manuals of the client components concerned.

- Which features the CMP has and how you operate it.

You find related information in the CMP product documentation.

- How to install and configure gateway components for using the features described here.

You find information about this in the product manuals of the gateway components concerned.

- Detailed configuration instructions for system components that are no OpenScape UC Application components.

This manual contains only guidelines for configuring such system components. These configuration guidelines describe the settings you need to perform. Such processes are explained in more detail in the configuration manuals of the system components concerned.

- How to manage, monitor, back up or restore system components that are no OpenScape UC Application elements.

You find information about this in the product manuals of the system components concerned.

2.3 Manual Structure

This manual is divided into the following chapters:

[Chapter 1, “About this Manual”](#)

This chapter contains general information about the manual itself. It helps you finding your way on the following pages and to quickly access important and useful information.

[Chapter 2, “Features with individual Configuration”](#)

This chapter introduces the OpenScape features the configuration of which is described in this manual.

[Chapter 3, “System Configuration”](#)

This chapter describes the steps for performing an OpenScape UC Application-based configuration of the communications solution.

[Chapter 4, “System Management for overlapping OpenScape Components”](#)

This chapter describes concepts and general tasks for managing the overlapping components of an OpenScape system.

[Chapter , “System management for the components of OpenScape UC Application”](#)

This chapter describes concepts and general tasks for managing the system components of OpenScape UC Application.

[Chapter 6, “System Monitoring”](#)

This chapter describes concepts and general tasks for monitoring an OpenScape system.

[Chapter 7, “Statistics Data”](#)

This chapter describes, which statistics data OpenScape UC Application can provide.

[Chapter 8, “Upgrading external Systems”](#)

This chapter describes configuration steps for the case that you upgrade an external system connected to OpenScape UC Application.

[Chapter 10, “Configuring a Certificate Strategy”](#)

This chapter describes how to configure an individual certificate strategy for the OpenScape system.

[Chapter 11, “IPsec Configuration”](#)

This chapter describes how to secure the communication between the UC Application systems with the IPSec protocol.

[Chapter 12, “Data Structure of the Domain Management Data”](#)

This chapter describes the structure of the domain administration data. This information will be of interest to you if you want to configure user data via the import feature of the CMP, for example.

[Chapter 13, “User Privileges for OpenScape UC Application”](#)

This chapter describes how the services of OpenScape UC Application are assigned to the user privileges in the UC Application user profiles.

[Chapter 14, “Voice Portal Settings in the CMP \(Voice Portal Plug-in\)”](#)

This chapter provides reference information about the voice portal plug-in, in which the voice portal access settings are performed.

[Chapter 15, “Conference Portal Settings in the CMP \(Conference Portal Plug-in\)”](#)

This chapter provides reference information about the conference portal plug-in, in which, among other things, the conference portal access settings are performed.

[Chapter 16, “General Properties for the Conference Portal”](#)

This chapter provides reference information about the conference portal.

[Chapter 17, “Managing the Conference Video Layout”](#)

This chapter describes how the video layout of conferences can be customized.

[Chapter 18, “Conference Management Tool Coman”](#)

This chapter describes how the conference management tool Coman can be used to manage the conferences of the conference portal independently from OpenScape UC Application and its clients.

[Chapter 19, “OpenScape Auto Attendant”](#)

This chapter describes the automated central postmaster AutoAttendant, which can be customized.

[Chapter 20, “Displaying Directory Numbers in the UC Application Clients”](#)

This chapter describes how the UC Application clients display telephone numbers – e. g. in the user’s call journal.

[Chapter 21, “Provisioning via LDAP Directories”](#)

This chapter describes an interface via which provisioning data can be copied from an LDAP directory to OpenScape UC Application.

[Chapter 22, “Adding an External Language in Integrated Simplex”](#)

This chapter describes how to add language specific packages for Integrated Simplex.

[Chapter 23, “Reverse Proxy”](#)

This chapter gives an overview of Reverse proxy.

[Chapter 24, “HAProxy Manager Tool”](#)

This chapter describes the new haproxymanager tool.

[Chapter 25, “Configuring Internet Access of OpenScape UC clients”](#)

This chapter describes the Internet access of OpenScape UC clients.

[Chapter 26, “Reverse Proxy deployment information”](#)

This chapter contains information about the Reverse proxy deployments

[Chapter, “IPv6 Support”](#)

This chapter describes the IPv6 configuration

2.4 General Conventions

With version 7 the product name HiPath 4000 changes to OpenScape 4000.

In this manual we use the product name OpenScape 4000 as synonym for both name variants. If information depends on the product version, we name the relevant product version explicitly.

2.5 Representation Conventions

To highlight information, we use the following markups and representations in this manual.

- [Text Markups](#)
- [Further Markups](#)
- [Representation of the Configuration Process – System Configuration](#)
- [Markups for Configuration Steps which Are Subject to Restrictions](#)
- [Representation of the Configuration Process – Certificate Strategy](#)

2.5.1 Text Markups

In this manual we use the following markups to highlight selected text passages.

For the following elements	Example
• Book title	<i>OpenScape UC Application Planning Guide</i>
• System entries and outputs • File names and system directory specifications • File contents	<code>conn %CONNECTION_NAME%</code>
• Menu names and entries in a GUI • Names of GUI entry fields • GUI buttons • GUI tabs • Names of keyboard keys • Highlighted names	Click on Save to ...
Specifications with individual content as a rule.	• C:\<user directory>\ • <address list>
Active cross reference for skipping to the specified passage in the manual.	• Text Markups • Chapter 1, “About this Manual”
Sequence of menu entries to be selected	Accounts > List

2.5.2 Further Markups

Critical notes and additional information are indicated in this manual in the following manner:

IMPORTANT: This indicates notes that carry information of **high priority**. Please definitely read and heed such notes to avoid malfunctions, loss of data or damages to devices.

NOTICE: Notes indicated in this way point to information worth knowing or useful tips.

2.5.3 Representation of the Configuration Process – System Configuration

In [System Configuration](#) on page 80, an illustration shows on each page the stage of the configuration process you have currently reached. This will help you to orientate in the described configuration process.

You can also use the illustrations to navigate in the configuration chapter. Simply click on the name of the configuration section you want to switch to. You immediately reach the first page of the selected section then.

The elements you see in the illustrated configuration process have the following meaning.

	Mandatory configuration steps You must perform these steps for the OpenScape system to operate smoothly.
	Optional configuration steps You need to perform these steps only if you want to use the relevant OpenScape feature.

2.5.4 Markups for Configuration Steps which Are Subject to Restrictions

In the configuration part of [System Configuration](#) on page 80, there are configuration steps described which must and may only be performed under certain circumstances. In such cases, an individual configuration restriction precedes the corresponding step in the step overview.

Example:

How to configure instant messaging:

1) For all deployment scenarios except for Very Large Deployment:

[Chapter , “Configuring the Openfire Server”](#)

2) For Integrated Deployment:

[Chapter , “Creating Packet Filter Rules in OpenScape Voice”](#)

3) Chapter , “Configuring the IM Address for OpenScape Users”

4) Chapter , “Creating and synchronizing Openfire User Accounts”

In this example, the configuration steps indicated must be executed as follows.

- Step 1 for all deployment scenarios except for Very Large Deployment.
- Step 2 only for Integrated Deployment.
- Step 3 and Step 4 in any circumstance

The configuration conditions in [System Configuration](#) on page 80 are not restricted to the deployment scenario used. There are also restrictions which apply e. g. to connected external systems.

Each configuration restriction is repeated as an introducing note in the corresponding configuration chapter.

2.5.5 Representation of the Configuration Process – Certificate Strategy

[Configuring a Certificate Strategy](#) on page 646 describes how to configure a certificate strategy for OpenScape UC Application. The configuration steps you need to take depend on the customer environment in which you use OpenScape UC Application.

[Configuring a Certificate Strategy](#) on page 646 defines four different customer environments – CE 1 to CE 4.

A graphic representation shows you in every configuration chapter of [Configuring a Certificate Strategy](#) on page 646 for which of these customer environments you need to execute the relevant configuration steps.

Example:

Execute these steps for:

CE 1	CE 2		

In this case you need to execute the steps of the relevant configuration chapter only if you use customer environment 1 or 2.

2.6 Specified Deployment Scenarios

In this manual we speak in particular of the following deployment scenarios, which always refer to OpenScape UC Application:

- Integrated Deployment
- Small Deployment
- Large Deployment
- Very Large Deployment

You find detailed information about these deployment scenarios of OpenScape UC Application in the *OpenScape UC Application, Planning Guide* manual.

If this manual ever mentions a deployment scenario not related to OpenScape UC Application but to another system, the relevant system and the deployment scenario is explicitly named. Detailed information about deployment scenarios of another system provides the product documentation of the relevant system.

2.7 Specified Default Passwords

In various passages of this manual we point to default passwords that are valid for preset system user accounts. These default passwords are preset for use during the setup of the relevant system and should immediately be modified by the administrator for security reasons.

A default password mentioned in the relevant manual passage may therefore not be valid any more and cannot be used to access the system.

In such a case you can obtain the current password from the administrator or from the person who has installed the system.

2.8 Acronyms used

In this manual we use the following acronyms.

Table 1: Acronyms used

Acronyms	Meaning
AD	Active Directory
API	Application Programming Interface
CA	Certificate Authority
CAD	Calling Number
CALEA	Communications Assistance for Law Enforcement Act
CMP	Common Management Platform
CSR	Certificate Signing Request
CSV	Comma-Separated Values
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
CWA	Communicator Web Access
DC	Domain Controller
DES	Data Encryption Standard
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
GPMC	Group Policy Management Console
GRUU	Globally Routable User Agent URI
GUI	Graphical User Interface
HPUM	HiPath User Management

Acronyms	Meaning
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification description
IIS	Internet Information Service
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
JAAS	Java Authentication and Authorization Service
KDC	Key Distribution Center
LDAP	Lightweight Directory Access Protocol
LVM	Logical Volume Manager
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MS	Microsoft
OND	One Number Device
ONS	One-Number Service
OS	OpenScape
OSILA	OpenScape Identity Life Cycle Assistant
OWA	Outlook Web Access
PE	Personal Edition of the OpenScape Desktop Client
PID	Permission ID
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RTP	Real Time Transport Protocol
SIP	Session Initiation Protocol

Acronyms	Meaning
SIP SM	SIP service manager
SPML	Service Provisioning Markup Language
SPN	Service Principal Name
SSL	Secure Sockets Layer
SSO	Single-Sign-on
TCP	Transmission Control Protocol
TCSPI	Telephony Conferencing Service Provider Interface
TK	Telecommunication
TLS	Transport Layer Security
TSE	Trusted Service Entry
TTM	Trusted transfer mode
TTS	Text-to-Speech
TUI	Telephony User Interface
UC	Unified Communications
UCMA	Unified Communications Managed API
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
WE	Enterprise Web Embedded Edition of the OpenScape Desktop Client
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XPR	OpenScape Xpressions

2.9 Continuative Documentation

You find a list of all OpenScape UC Application manuals in the manual *OpenScape UC Application, System Description*.

2.10 Data Protection and Data Security

This system also processes and uses personal data for purposes such as billing, displays, and customer data acquisition.

In Germany, the processing and use of such personal data is subject to various regulations, including the regulations 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 being 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.

NOTICE: The customer is responsible for ensuring that the system is 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.

Members of the Unify GmbH & Co. KG are required to observe business and data secrecy as a result of the company's work rules.

In order to ensure that the statutory requirements during service – whether during “on-site service” or during “remote service” – are consistently met, you should always observe the following rules. You will not only maintain 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; do not allow unauthorized persons to gain access to passwords by writing them down on a piece of paper or via other means.
- 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 diskettes 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.

3 Features with individual Configuration

You need to individually configure the following OpenScape UC Application features after the system installation for using them.

- [One-Number Service \(ONS\)](#)
- [The Conference Portal](#)
- [The Voice Portal](#)
- [Microsoft Exchange Connection](#)
- [IBM Lotus Domino Connection](#)
- [LDAP Connection](#)
- [Instant-Messaging Connection](#)
- [OpenScape Xpressions Connection](#)
- [Networking Deployment Scenarios](#)
- [Presence Status in VCard](#)
- [Outlook contact picture is not shown in UC](#)
- [Using Chat History](#)
- [Outlook Extension / Fusion for Office - add Grace period for calendar](#)
- [Voicemail tab for UC WebClient and Fusion for Office / Notes](#)
- [New Voice Mail Greeting Feature \(UCMODE\)](#)

The following sections provide an overview of these services.

3.1 One-Number Service (ONS)

The one-number service combines all phone numbers under which an OpenScape user can be reached.

Combining phone numbers has the following advantages.

- For each OpenScape user only a single phone number, under which he/she can be reached, must be published – the ONS number.
- At any time, each OpenScape user can choose in his/her UC Application client the device he/she would like to assign the ONS phone number to – the preferred device (OND).
- If an OpenScape user receives a call under his/her ONS phone number, this call is always directly forwarded to the preferred device (OND). If the call is not accepted there, the device is busy or the connection disturbed, the call is forwarded to other possibly available terminals of the OpenScape user in succession. The order in which the devices are used is defined by the OpenScape user via an individual device list. When trying the devices on the list in succession, engaged devices are skipped by default.

No matter on which device the OpenScape user accepts the call: The caller will always see the ONS number of the called OpenScape user.

NOTICE: The skipping of engaged devices can be prevented by using the Busy-on-Busy feature. In this case, the caller hears a busy signal if the call is routed to an engaged device. The routing to possible further devices is subsequently canceled. The phone number of the engaged device is displayed to the caller.

- When the OpenScape user initiates a phone call from his/her selected preferred device (OND), the ONS phone number of the OpenScape user is displayed to the callee as originator number.

The one-number service does not take effect in the following cases:

- If the OpenScape user is called under a number different from his/her ONS number.
- If the OpenScape user initiates a call from a device he/she has currently not selected as preferred device (OND).

IMPORTANT: When an incoming call is diverted to the preferred device the call control window in the WebClient can only be accessed in the ONS device. That is, the call control window cannot be accessed via the preferred device's WebClient.

3.1.1 Interworking with Multi-Line Hunt Group (MLHG)

In case you have MLHG-members and it is required that they can set a preferred device list or their voice mail as preferred device then the OpenScape Voice services Computer Supported Telephone Adapter (CSTA) and One Number Service (ONS) must be configured for the subscriber of the MLHG and also to the pilot of the MLHG group.

3.2 The Conference Portal

The conference portal provides virtual conference rooms in which users can gather and hold audio and video conferences.

You find a detailed conference portal feature description in the *OpenScape UC Application, System Description* manual.

3.3 The Voice Portal

The voice portal provides a telephone user interface (TUI) via which users can access the comprehensive Unified Communications services of OpenScape UC Application. The user operates this telephone user interface via the keypad of his/her telephone or by voice commands.

There are two applications for the voice portal, each of them providing different telephone user interfaces:

- The Voice Portal application

This application provides telephone user interfaces that a user operates via his/her telephone's keypad.

- The application Voice Portal "Speech"

This application provides telephone user interfaces that a user operates by voice commands.

Features with individual Configuration

Microsoft Exchange Connection

Each of the voice portal applications Voice Portal and Voice Portal "Speech" provide two access types of telephone user interfaces that enable accessing the respective voice portal application:

- The user access (control mode)
OpenScape users can deploy an access of this type to, for example, configure their UC Application settings or access the Unified Communications services of OpenScape UC Application.
- The guest access (answering machine mode)
Guests can use an access of this type to leave messages for OpenScape users.

Voice portal application profiles

You can perform the settings of the voice portal applications Voice Portal and Voice Portal "Speech" specific to the Media Server in the voice portal plug-in of the CMP. This configuration is based on voice portal application profiles. Using a terminal you can bind each of these application profiles to access numbers, thus realizing voice portal accesses with individual settings.

You find a detailed voice portal feature description in the *OpenScape UC Application, System Description* manual.

3.4 Microsoft Exchange Connection

You use the Microsoft Exchange connection to connect the OpenScape system to a Microsoft Exchange system. This connection is based on the groupware connector of OpenScape UC Application, which accesses the Microsoft Exchange system via a technical user account.

The OpenScape system supports the connection of Microsoft Exchange Server 2013, 2016 and 2019 via the groupware connector.

The Groupware-Exchange connector does not directly access the user data of Microsoft Exchange servers.

- For Microsoft Exchange 2013 / 2016 / 2019, the Groupware-Exchange connector connects to the Microsoft Exchange system via a Client Access Server (CAS server) and the Microsoft Exchange Web Services.

The Groupware-Exchange connector connects to the Microsoft Exchange System either unsecured via HTTP or secured via HTTPS. In case of secured communication it uses the SSL protocol. Furthermore, you can configure an authentication procedure for the Groupware-Exchange connector communication.

In operation, OpenScape UC Application creates e-mails independently and sends them to the e-mail inboxes of the Microsoft Exchange system. The Groupware-Exchange connector sends such anonymous e-mails via an SMTP server, which forwards them accordingly. The SMTP server works independently from OWA Server or Client Access Server / Microsoft Exchange Web Services.

A Microsoft Exchange connection offers OpenScape users the following advantages:

- Voice messages are stored in the Microsoft Exchange inbox of the addressed OpenScape user.
- OpenScape users can access their Microsoft Exchange inbox via voice portal and execute the following tasks:
 - Playing /deleting /restoring messages
 - Marking messages as read/unread.
 - Answering/forwarding messages with a voicemail
 - Creating new voicemails
- OpenScape users can access their Microsoft Exchange calendar via voice portal and execute the following tasks:
 - Playing / accepting /declining appointments
 - Sending a voicemail to the appointment initiator
- OpenScape users can access their private Microsoft Exchange contacts with their UC Application client and execute the following tasks:
 - Creating /deleting /modifying/searching for contacts

The private contacts of the UC Application clients are in this case no longer stored in the OpenScape system but in the contact folder of the Microsoft Exchange inbox.

Contacts are regularly synchronized between the UC Application clients and the Microsoft Exchange system. The deletion of a contact on the outlook appears on the client within a day.

IMPORTANT: If the contact management is migrated from the internal OpenScape-based solution to the Microsoft Exchange inbox, no contacts are synchronized that are already present in the OpenScape system.

NOTICE: You can configure the Microsoft Exchange connection also in such a way that the OpenScape users' access to their private Microsoft Exchange contacts is restricted to reading.

3.5 IBM Lotus Domino Connection

You connect an IBM Lotus Domino 8.5.x or 9.0.x server to the OpenScape system via the IBM Lotus Domino connection. This connection is based on the groupware Domino connector of OpenScape UC Application.

The groupware Domino connector does not directly access the user data of the productive IBM Lotus Domino server (groupware server). Instead, it accesses a Notes API, which you install on the OpenScape UC Application computer system with an IBM Lotus Domino server (connector server). This Notes API then uses a technical user account to connect to the groupware server.

The connector server is exclusively used to establish the connection between the OpenScape system and the productive IBM Lotus Domino network. It is not integrated as IBM Lotus Domino server in the productive IBM Lotus Domino network.

An IBM Lotus Domino connection offers OpenScape users the following essential advantages:

- Voice messages are deposited in the IBM Lotus Domino inbox of the addressed OpenScape user.
- OpenScape users can access their IBM Lotus Domino inbox via voice portal and execute the following tasks:
 - Playing /deleting /restoring messages
 - Marking messages as read/unread.
 - Answering/forwarding messages with a voicemail
 - Creating new voicemails
- OpenScape users can access their IBM Lotus Domino calendar via voice portal and execute the following tasks:
 - Playing / accepting /declining appointments
 - Sending a voicemail to the appointment initiator
- OpenScape users can access their private IBM Lotus Domino contacts and execute the following tasks with their OpenScape Web Client or their OpenScape Desktop Client:
 - Creating /deleting /modifying/searching for contacts

To enable an OpenScape user managing his/her IBM Lotus Notes contacts in the OpenScape clients, one of the following requirements must be complied with.

- The OpenScape user has been created in the IBM Lotus Domino server as roaming user. This is done by the IBM Lotus Notes administrator. A roaming user can access his/her individual IBM Lotus Notes client environment from different IBM Lotus Notes clients.
- The OpenScape user's private address book must have been stored on the IBM Lotus Domino server. The user needs to configure this private-address-book replication by himself/herself. User often have already configured this function for retrieving their data via the IBM Lotus Notes web access.

NOTICE: While the groupware connector of OpenScape UC Application enables accessing private Domino contacts, DirX or Tivoli realize additional access to global Domino contacts. DirX is not needed if Tivoli Identity Management is available for your system. Professional Services & Solutions (PS & S) of Unify Software and Solutions GmbH & Co. KG will deliver DirX and then complete the individual integration and configuration for DirX on your system.

NOTICE: Due to a picture format restriction in Domino Server, users are suggested to define the photos of their contacts via Domino Notes Client/Administrator and not from OpenScape UC WebClient. The contact photos will be retrieved in WebClient by querying Domino Server.

3.6 LDAP Connection

Via the LDAP connection you connect the OpenScape system to external LDAP directories. In this way you can provide an LDAP-based global contact list to OpenScape users, for example.

The LDAP connection is based on the OpenScape UC Application directory service, which supports a general LDAP-based search feature. But entries of a connected directory can neither be created nor modified or deleted from within the OpenScape system.

Via the LDAP connection the OpenScape system can also be connected to an Active Directory. Such a connection does not allow access to global contact lists in Microsoft Exchange, though.

3.7 Instant-Messaging Connection

You can connect the OpenScape system to an Instant Messaging server via the XMPP protocol. This enables OpenScape users to communicate with other users via Instant Messaging connections.

If OpenScape UC Application is connected to an Openfire server, the IM media presence status of OpenScape users is displayed in the OpenScape clients. OpenScape UC Application determines this IM media presence status from whether or not an OpenScape user is logged in at the Openfire server.

NOTICE: An Openfire server and Microsoft Lync cannot both be connected to OpenScape UC Application.

NOTICE: An incorrect presence status may be displayed if an OpenScape user connects to the Openfire server via different clients simultaneously. The Openfire server does not yet support such log-in scenarios.

NOTICE: The access passwords for OpenScape users are exclusively administered under OpenScape UC Application. Passwords on the Openfire server are not considered. If an OpenScape user deploys an IM client alien to the system and changes his/her access password, only the password stored on the Openfire server changes. Consequently, there are two different passwords: The password under OpenScape UC Application and the one in the Openfire server. These two are not automatically synchronized. In this case the user needs to log on to OpenScape clients with the first password and to IM clients alien to the system with the second.

IMPORTANT: When using the instant messaging feature, make sure that the same NTP server is used in both the UC

and Openfire servers, in order to synchronize the time between them.

3.8 OpenScape Xpressions Connection

This chapter provides information about the following topics:

- [OpenScape Xpressions Connection Overview](#)
- [Working Method of the OpenScape Xpressions Connection](#)
- [Calling Number Schema](#)
- [Restrictions on the OpenScape Xpressions Connection](#)

3.8.1 OpenScape Xpressions Connection Overview

You can use the OpenScape Xpressions connection to connect the PhoneMail application of XPR servers to OpenScape UC Application. Such a connection extends the Unified Messaging features of the PhoneMail application by the Unified Communications features of OpenScape UC Application.

When you connect an XPR server to OpenScape UC Application via the OpenScape Xpressions connection, the Unified Communications features of OpenScape UC Application integrate in the PhoneMail user menu of the XPR server. The XPR user will not realize whether a selected feature is enabled by the XPR server or by OpenScape UC Application. He/she will receive the impression as if working with a Unified Communications system centrally providing all available features.

You can connect several OpenScape Xpressions systems to several UC Application systems with any assignment ($m \times n$ connection).

3.8.2 Working Method of the OpenScape Xpressions Connection

The OpenScape Xpressions connection communicates via the default protocol IP. If an XPR user logs on to the PhoneMail application and uses an OpenScape UC Application feature in there, the XPR server routes the call of the XPR user to the user access of the voice portal. There, the XPR user is automatically authenticated without any further inputs required. Subsequently, the user menu associated to the selected feature will be directly announced to the XPR user under OpenScape UC Application.

The XPR server transfers various information to OpenScape UC Application along with the call. The XPR server encodes this information in the originator number of the forwarded call, using the Trusted Transfer Mode (TTM) phone number format for the encoding.

The TTM phone number format has the following general structure:

<Start character> <Trusted domain> <Original system> <User information>

Also the Endpoint Attribute "SEND ALPHANUM SIPURI WHEN AVAIL" must be set. (Either via startCli or via Assistant / CMP).

The various TTM phone number format elements specify the following:

- **Start character**

The start character is an indicator for the XPR and UC Application components involved to recognize the relevant phone number as a number in TTM phone number format.

The start character can be, for example, the * character or any other non-numerical character

Trusted domain

Specifies the ID of the system that has created the relevant phone number. This ID is evaluated by the system that receives the information. Forwarded calls with invalid ID will not be accepted by the receiving system.

Original system

The original system defines from which system the trusted transfer was induced.

- From the XPR server, if an XPR user switches under PhoneMail to OpenScape UC Application features.
- From OpenScape UC Application if the XPR user returns to the PhoneMail features.

User information

The User Information specifies:

- The original phone number of the user in localized format (ANI)

NOTICE: The ANI is always handed over in the E.164 format.

- The user's voice box number (user ID)
- The TUI entry point in the original voicemail system
- The user language

The calling number schema determines the format of the various elements of the TTM phone number format (cf. [Calling Number Schema](#) on page 37).

3.8.3 Calling Number Schema

If a call is forwarded as trusted transfer from the XPR server to OpenScape UC Application or vice versa, various information must be exchanged between XPR server and OpenScape UC Application with the forwarding (cf. [Working Method of the OpenScape Xpressions Connection](#) on page 36). The calling number schema specifies in which format this information is exchanged.

The calling number schema consists of several consecutive sections. Each of these sections defines the format of an element of the phone number format.

The notation of these sections depends on whether you view the calling number schema on the OpenScape UC Application side or on the XPR server.

Notation for OpenScape UC Application

The calling number schema consists on the OpenScape UC Application system side of several consecutive sections of the following format:

p<[Argument Index](#)> v<[Argument Length](#)>

The different elements of a section define:

- **Argument Index**

A running number that serially numbers the different consecutive arguments of the user information.

- **Argument Length**

The permanent number of digits contained in the relevant argument.

Notation for XPR Server

The calling number schema consists on the XPR server side of several consecutive sections of the following format:

%<Argument Index> \$<Argument Length>

The different elements of a section define:

- **Argument Index**

A running number that serially numbers the different consecutive arguments of the user information.

- **Argument Length**

The number of digits used for the relevant argument.

Only the first section of the calling number schema deviates from this format. This first section always describes a single character – the start character (S). The start character must be prefixed with a p.

Example:

Permanently defaulted phone number format:	<S><TD><ORG><ANI><UID><OTUI><LNG>
Calling number schema (OpenScape system):	p0v1p1v1p2v1p3v13p4v4p5v2p6v1
Calling number schema (XPR server):	p*%1 \$1 %2 \$1 %3 \$13 %4 \$4 %5 \$2 %6 \$1
Transferred originator number	*9055485548616

Decoded this results in:

• p0 / p*:	Start character (S)	:	*
• p1 / %1:	Trusted Domain (TD)	:	9
• p2 / %2:	Original system (ORG)	:	0
• p3 / %3:	ANI	:	4924040901100

NOTICE: The ANI is always handed over in the E.164 format.

• p4 / %4:	User ID (UID)	:	5548

NOTICE: The user ID corresponds to the voicebox number as it is entered for the relevant user in the **VOICE#** database field of the XPR Correlation Database. In a TTM system environment this number may be of different length for the respective users.

In this case the longest of possible user ID lengths must be configured for the user ID argument in the calling number schema.

• p5 / %5:	Original TUI User Entry Point (OTUI)	:	61
• p6 / %6:	Language (LNG) - If you use one of the following languages you need to configure at least length 1 for this argument: - German (Trace ID = 0) - English (UK) (Trace ID = 1) - French (Trace ID = 2) - Italian (Trace ID = 3) - Spanish (Trace ID = 4) - Dutch (Trace ID = 5) - English (US) (Trace ID = 6) - If you use one of the following languages you need to configure length 2 for this argument: - Portuguese (Portugal) (Trace ID = 10) - Portuguese (Brazil) (Trace ID = 11) - Spanish (US) (Trace ID = 12) - French (Canada) (Trace ID = 13) - Russian (Trace ID = 14) - Turkish (Trace ID = 15) - Czech (Trace ID = 16) - Japanese (Trace ID = 17) - Slownian (Trace ID = 18) - Polish (Trace ID = 19)	:	6

NOTICE: If the transferred language is unavailable for the voice portal, the voice portal TUI is played in the language configured for the relevant voice portal access as default language.

In the example, argument length **4** is configured for parameter 3 (**p3** or **%3**) – the example thus works with four-digit extension numbers.

If you want to use a different length for the extensions you need to configure a different argument length for the parameters 3 and 4. In doing so please note that the total length of the phone number expression must normally not exceed

Features with individual Configuration

a maximum length. This length is defaulted by the communications system used.

NOTICE: Maximum lengths for the phone number expression:

- OpenScape Voice: 24 characters
 - OpenScape 4000: 22 characters
-

Examples of calling number schemas with different extension lengths:

Extension length	UC Application system	XPR Server
Three-digit	p0v1p1v1 p2v1 p3v13 p4v 3 p5v2 p6v1	p*%1\$1 %2\$1 %3\$13 %4\$ 3 %5\$2 %6\$1
Four-digit	p0v1p1v1 p2v1 p3v13 p4v 4 p5v2 p6v1	p*%1\$1 %2\$1 %3\$13 %4\$ 4 %5\$2 %6\$1
Five-digit	p0v1p1v1 p2v1 p3v13 p4v 5 p5v2 p6v1	p*%1\$1 %2\$1 %3\$13 %4\$ 5 %5\$2 %6\$1

NOTICE: When you change the calling number schema you need to perform this modification for OpenScape UC Application as well as for the XPR server.

3.8.4 Restrictions on the OpenScape Xpressions Connection

For the OpenScape Xpressions connection please note the following:

- The XPR server and OpenScape UC Application must be connected to the same communications system.

NOTICE: For the time being, the Trusted Transfer Mode has only been approved for usage at the communications systems OpenScape Voice and OpenScape 4000.

3.8.5 Simultaneous availability of WebAssistant and the Voice Mail tab in WebClient

In WebClient, the Voice Mail tab is available by clicking the respective button on the left side and the WebAssistant is available via the user **photo > Settings > General tab > Voice mail configuration > Configure your voice mail here**.

Please refer to [Nuance services to be verified to allow simultaneous availability of WebAssistant and the Voice Mail tab in WebClient](#) on page 297.

3.9 Networking Deployment Scenarios

With Very Large Deployment you can install OpenScape UC Application with several networked clusters for providing the UC Application services to a maximum number of users.

If required, all other deployment scenarios of OpenScape UC Application can be networked with help of the Openfire system's Federation functionality also. This is useful, for example, to connect UC Application environments operated separately so far in the scope of a company merger, thus providing the users of both UC Application environments with presence information.

You find details of the deployment scenario networking concept in the *OpenScape UC Application, Planning Guide* manual.

3.10 Proxy-based Login

Proxy-based login is used to securely authenticate users by delegating the process of authenticating Web Client users to a proxy server. This proxy server is configured to intercept the communication between clients and the Web Client, i.e. the FQDN in the published Web Client URL resolves to the proxy server's IP address and not to the Web Client itself. The proxy authenticates users securely and passes the user's validated ID in a proprietary HTTP header line when forwarding the request to the Web Client.

The proxy-based authentication is only performed when a client accesses the login URL. Subsequent requests during the same session are authenticated by session cookies.

In case of multiple Web Client Front-End servers, the proxy server can be configured to distribute sessions over the available Front-End servers, i.e. it could act as a load balancer. Alternatively, a separate load balancer can be placed between the proxy server and the Web Client servers. It is suggested to set up a load balancer fronting the Web Client servers, which can be configured to send requests for the login URL through the proxy.

The Web Client login URL may only be reached through the proxy via a suitably configured firewall or network setup, in order to ensure the system's security. In addition, the proxy must strip the selected HTTP header line from any inbound HTTP request.

When the Web Client receives a HTTP request including the proprietary HTTP header line, it uses its provisioned data to translate the "external" ID passed by the proxy to the "internal" OpenScape user ID and considers the user authenticated if the translation was successful. If the HTTP header line is not present, or no OpenScape user can be found for the received "external" ID, authentication is unsuccessful and the web browser displays either the default login screen, or a "login failed" screen, depending on configuration.

The proxy must fail authentication requests without assertion or authentication cookie with a "401 Unauthorized" response, containing the proprietary "X-Unify- Redirect" header line whose content must be the URL of the Assertion Consumer Service (i.e. the URL to redirect the browser to).

3.11 Presence Status in VCard

VCard is the contact card in Fusion for Office embedded in Outlook 2010 / 2013 / 2016.

All Vcard instances displayed in MS office e.g. Outlook email participants preview pane and open email, calendar invitations, people, hover Vcard window, search people, etc. will provide the user presence for all UC users that allow everybody to see their presence. Presence changes will be displayed automatically for the vCards opened or in focus.

So when you change the presence status in WebClient or SmartClient the change be seen in the VCard, Fusion for Office and also when you change the presence status from Fusion for Office you can see the change in WebClient and SmartClient.

NOTICE: The presence status is seen only when you allow others or specific people to see your presence state.

NOTICE: The profiles SmartClient rules and Standard Profile are automatic profiles created for imported rules, when you migrate from previous versions. If you unassign the rules associated with these profiles, the profiles will be automatically hidden and not be available any more.

3.12 Outlook contact picture is not shown in UC

When searching for contacts in UC the contact picture from Outlook cannot be retrieved and thus is not shown. However with V11 or Fusion V1.5.xxx or higher it is possible to retrieve the picture.

3.13 Using Chat History

With V11 one-to-one and group chats that have been previously exchanged can be retrieved and displayed on the users' UC clients.

This requires an Openfire Server to be external with its own MySQL Database and the Archiving feature enabled.

For Simplex, Small and Large deployments the Openfire server must be migrated to an external server (if not already external) and must be preconfigured from scratch with MySQL database which would be installed on the same server as Openfire (please see Installation and Upgrade Guide, section "Networked Openfire for Integrated Deployment, Small Deployment and Large Deployment"). The presence service setting "Deployment Mode" must be changed to "Openfire".

For Very Large Deployments only the Archiving feature need to be enabled.

To enable Archiving follow the instructions on this guide under [Activating IM Communication Archiving](#) on page 271. A restart of the Openfire Server is required for changes to take effect.

By default the chat history is kept for 365 days and users can retrieve their chat messages for the last 14 days.

The feature is only supported in deployments where Openfire is used as the Presence Provider.

IMPORTANT: Chat history in a networking/federated scenario is not supported.

3.14 Outlook Extension / Fusion for Office - add Grace period for calendar

There are two internal states for UC presence.

- In a Call
- In a Meeting

These internal states can only be taken when the user has the presence state "available".

For Outlook Appointment only the internal state "In a Meeting" is of interest.

Use Case:

- There is a scheduled conference in Outlook calendar:
User dials to the conference before the presence changes to the internal state "in a meeting". (From presence state "Busy" it will not be changed to "in a meeting")

There maybe other use cases as well.

The new parameter forces:

- The presence synchronization component will effectively consider Outlook Appointments to start 'graceperiod' milliseconds earlier than the actual schedule time, so that the internal state "In a Meeting" can be taken prior the state "Busy".

The new parameter is:

AppointmentGracePeriod (integer, milliseconds)

By default this parameter is zero.

Also when the parameter is not defined, it is consideres as zero.

The parameter is defined (or can be defined) in the XML-file

%appdata%\Unify\UCSolutions\office-configuration.xml.

(you can find the %appdata% when you go to the Command-prompt (cmd.exe) and enter **echo %appdata%**.

```
</ConfigurationData>
....
<AppointmentGracePeriod>0</AppointmentGracePeriod>
...
</ConfigurationData>
```

3.15 Voicemail tab for UC WebClient and Fusion for Office / Notes

With UC V11 it is possible to record greetings, so when calls are redirected to the voicemail box the caller gets a greeting.

IMPORTANT: A project-specific release is required to activate this feature.

There are various greetings available:

- default greeting
- single greeting
- vacation greeting
- business greeting

About the greetings you will find more information in the user guides (either UC WebClient or Fusion for Office / Notes)

The following preparation steps are needed:

1) update Xpression server to the latest hotfix

Check release notes

2) update Xpressions database

- greetings must be set to default system greetings
- configuration must be done on the Xpressions server by the Xpressions administrator.

NOTICE: You will find useful information and hints about the database configuration in the release notes.

3.16 New Voice Mail Greeting Feature (UCMODE)

A new Voicemail greeting interface has been introduced in OpenScape UC V11 WebClient and Fusion for Office V2 which enables users to configure the way that they have access to their VM greetings.

The UC users have the option to either use the new greetings mode or not depending on their individual configuration.

You can either:

- Set a more user friendly interface for the settings of voicemail greetings
- Choose to have voicemail settings with advanced configurations
- Remain in Xpressions mode
- Decide to use the UC mode
- Disable a user's voice mailbox
- Disable the user's voicemail access.

Features with individual Configuration

Parameter	Name	Meaning
U	UC mode	Users will be able to record all types of VM greetings defined in UC (Default, Single, Vacation and Business). This is the option recommended for new installations. Compared to Xpressions mode, it provides a more user-friendly UI for the basic settings of VM greetings.
X	Xpressions mode (default)	Users will be able to access the full set of settings for voice mail functionality, including all different VM greetings as defined in Openscape Xpressions. This option is the default option fully compatible with all previous versions. It is the option recommended for existing installations that do not want to have changes in the current VM greetings functionality. Compared to UC mode, it provides advanced configurations.
O	Xpressions mode with option to UC	Users will remain in Xpressions mode, but they may decide by their own to use the UC mode. This is the option recommended for old installations where the administrator wants to provide a new way for VM greetings configuration without forcing users to use it. Once users decide to use the UC mode, the users are switched to mode N (described below) and a backup of Xpressions configuration is automatically done to allow the rollback.
N	UC mode with option to Xpressions	This option should not be used for the initial configuration of the users. Users will be set automatically to this status as described above (mode O). If the users decide not to use the Xpressions mode anymore, then users are automatically set to mode U, but the administrator may give this option back to the users via using this parameter with Infotool.
D	No access	No access to VM greeting via UC webclient is given for the users. All greetings are defined by the administrator or users will have to access Xpressions Webassistant directly.

3.16.1 New Voice mail Greetings Activation in WebClient and Fusion for Office

It is mandatory to update the UC server to the Fix Release version: UC V9R4 FR11 or higher.

After that, the 'UseNewVmSettings' parameter must be set to "true" in order to activate the New Voice mail Greetings:

- Update the WebClientUI.cfg file in OSC UC Server backend with the following entry, located in the following path: /opt/siemens/HiPathCA/config/common

```
#
# Set this entry to 'true' to use the new, simplified
# Voicemail settings UI; otherwise, the old Xpressions link is
# displayed
#
UseNewVmSettings = true
```

NOTICE: OSC UC Server must be restarted in order to the changes take effect.

- No registry key is needed for Fusion for Office machines, but Fusion for Office has to be restarted to this configuration take effect.
- Clear browsing data should be done in the Web browsers or a webpage refresh to this configuration takes effect in the WebClient.
- Once WebClientUI.cfg parameter UseNewVmSettings is set to true, it is mandatory to install the Xpressions V7R1 FR5 HF25 P900 described in subchapter 1.2.1.

3.16.2 UC Voice mail modes

The Default mode can be access via the the OpenScape Xpressions Web Assistant by selecting Configure your voice mail here.

You can change your VM Greeting mode in OpenScape UC WebClient via the Settings > Voice mail tab.

3.16.2.1 How to change to new Voice mail Greetings mode

You, or your system administrator can change the VM Greeting mode (UC MODE) using one of the following ways:

- Via Openscape UC Settings Voicemail tab (detailed below)
- Via Openscape CMP User template sync with Xpressions (HpmApl)
- Via Openscape Xpressions Infotool using UCMODE parameter

For detailed information regarding CMP usage and user sync using Xpressions Template please refer to:

OpenScape Common Management Platform, Administrator Documentation.

For detailed information regarding Openscape Xpressions Infotool usage please refer to:

OpenScape Xpressions V7, Server Administration, Administrator Documentation.

3.16.2.2 How to change the user profile to 'Default system settings' for all users' voicemail boxes:

Although this is not mandatory, it is highly recommended to change all the users to the 'default system settings' before migrating from the old voicemail mode to the New Voice mail Greeting mode. This will allow the users to start using UC greetings mode.

This change can be done using Openscape Xpressions Infotool and setvmset parameter.

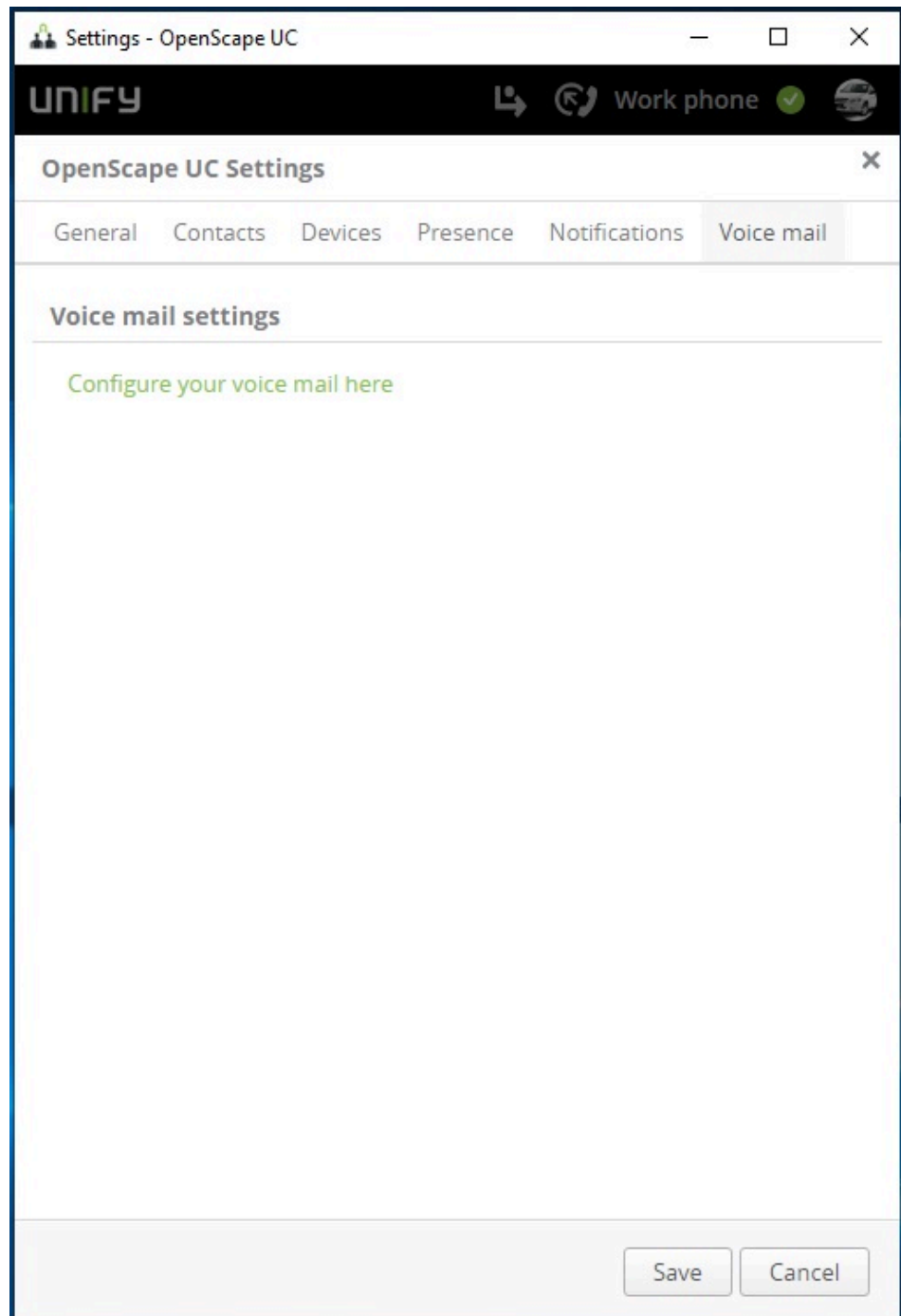
For more detailed instructions on using Openscape Xpressions Infotool, please refer to

OpenScape Xpressions V7, Server Administration, Administrator Documentation.

3.16.2.3 Default Mode (UCMODE = X)

If OpenScape Xpressions Administrator does not change the mode in the Xpressions Server after updating Xpressions to version V7R1 FR5 HF25 P900, the default mode for all users will be the Xpressions Voice mailbox UCMODE = X. That means, in other words, that the compatibility mode will be set for all users.

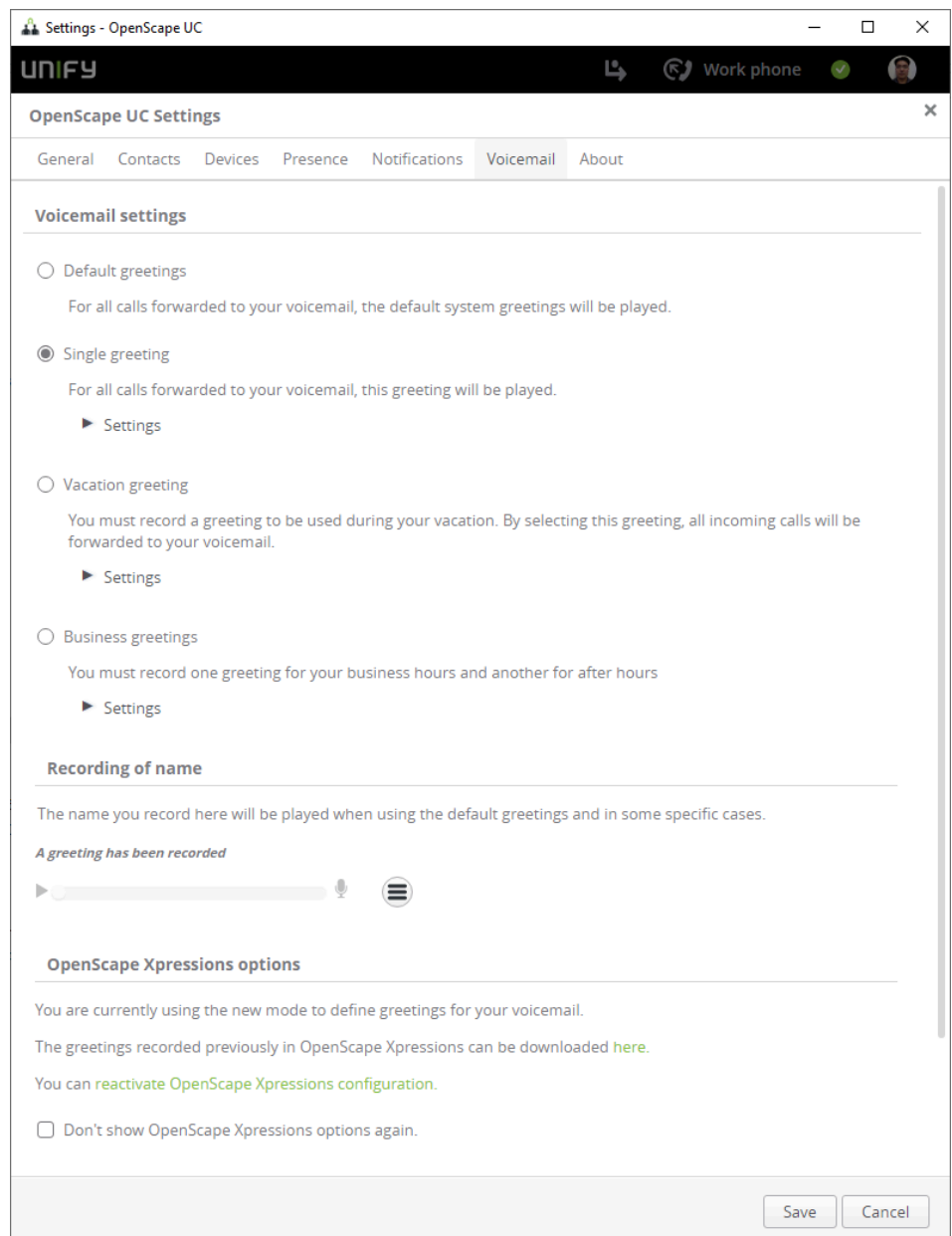
In the Default mode, the Voice mail tab will contain the following clickable text link: Configure your voice mail here that redirects you to OpenScape Xpressions WebAssistant.



3.16.2.4 New Greetings Mode (UCMODE = U)

For new UC server installations or new OpenScape Xpressions mailbox users, it is recommended to use the New Greetings mode without the OpenScape Xpressions option (UCMODE=U).

In this mode, the Voicemail tab is displayed as in the figure below:



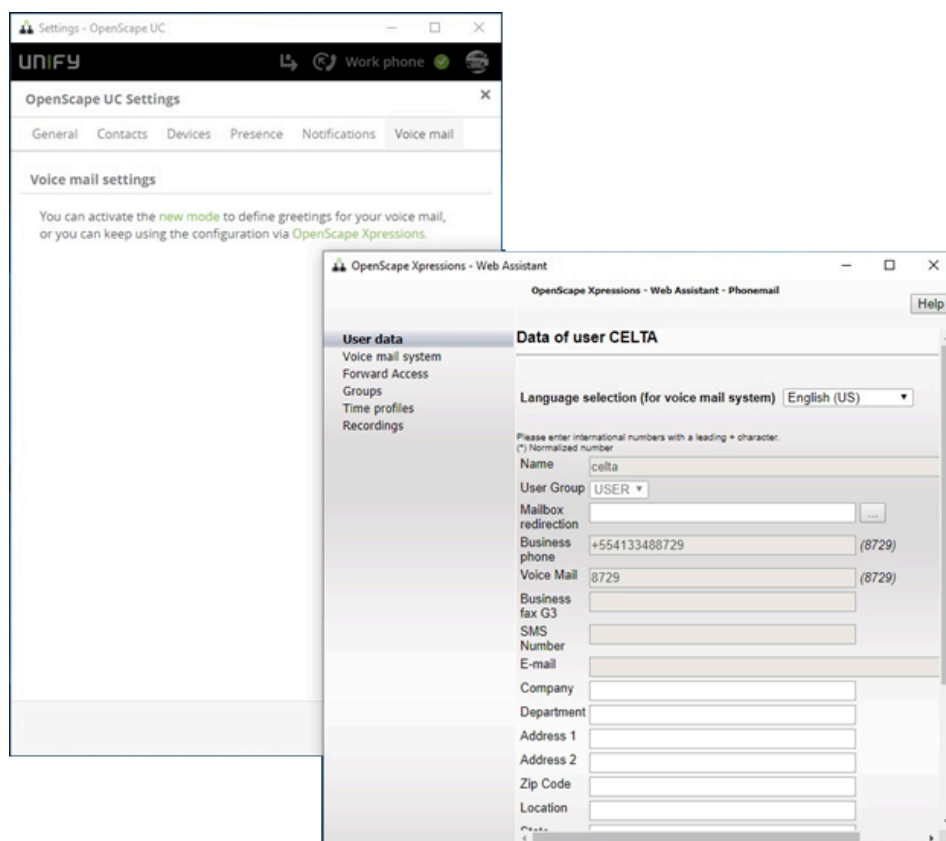
3.16.2.5 OpenScape Xpressions Mode with the option to change to New greetings mode (UCMODE = 0)

It is also possible to offer to each user the possibility to decide which mode to use,

i.e. continue using the advanced OpenScape Xpressions mode or try the new simple way to configure the voice mail greetings (UCMODE=0).

In this mode, the Voicemail tab is displayed as in the figure below:

Features with individual Configuration



The User can continue accessing the OpenScape Xpressions WebAssistant to configure the Voice mail settings by clicking the OpenScape Xpressions link or can try the New Greeting mode by clicking the new mode link.

NOTICE: Old voice mail settings (time profile, recorded greetings, etc) will be backed up and can be restored if the user decides to reactivate the OpenScape Xpressions mode.

The old greeting will be mapped to the new mode single greeting only if Personal Alternate greeting is previously set for all days of the week.

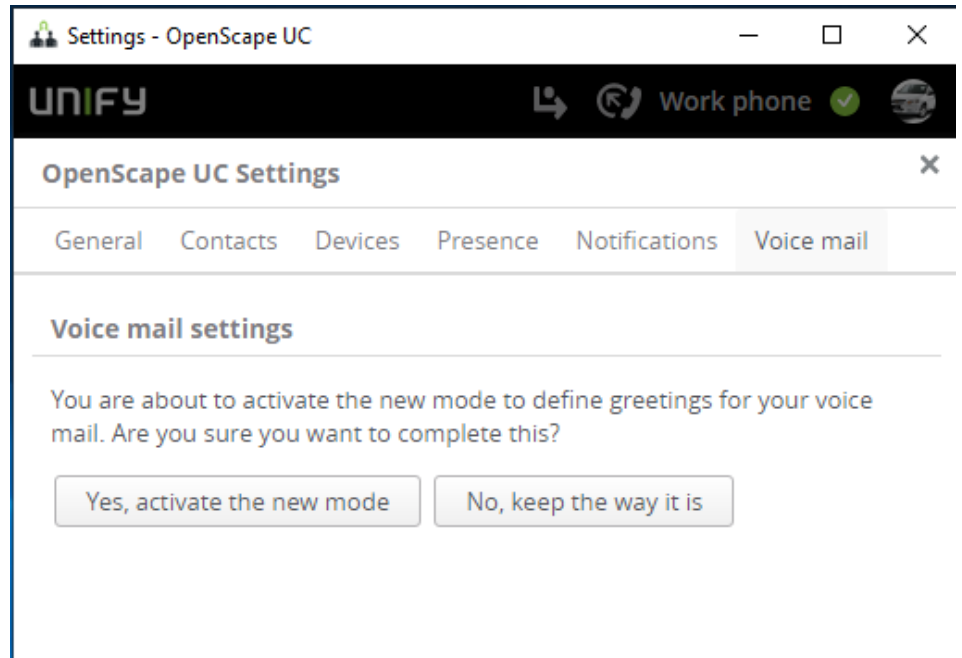
3.16.2.6 New Greetings Mode with reactivation option to OpenScape Xpressions Mode (UCMODE = N)

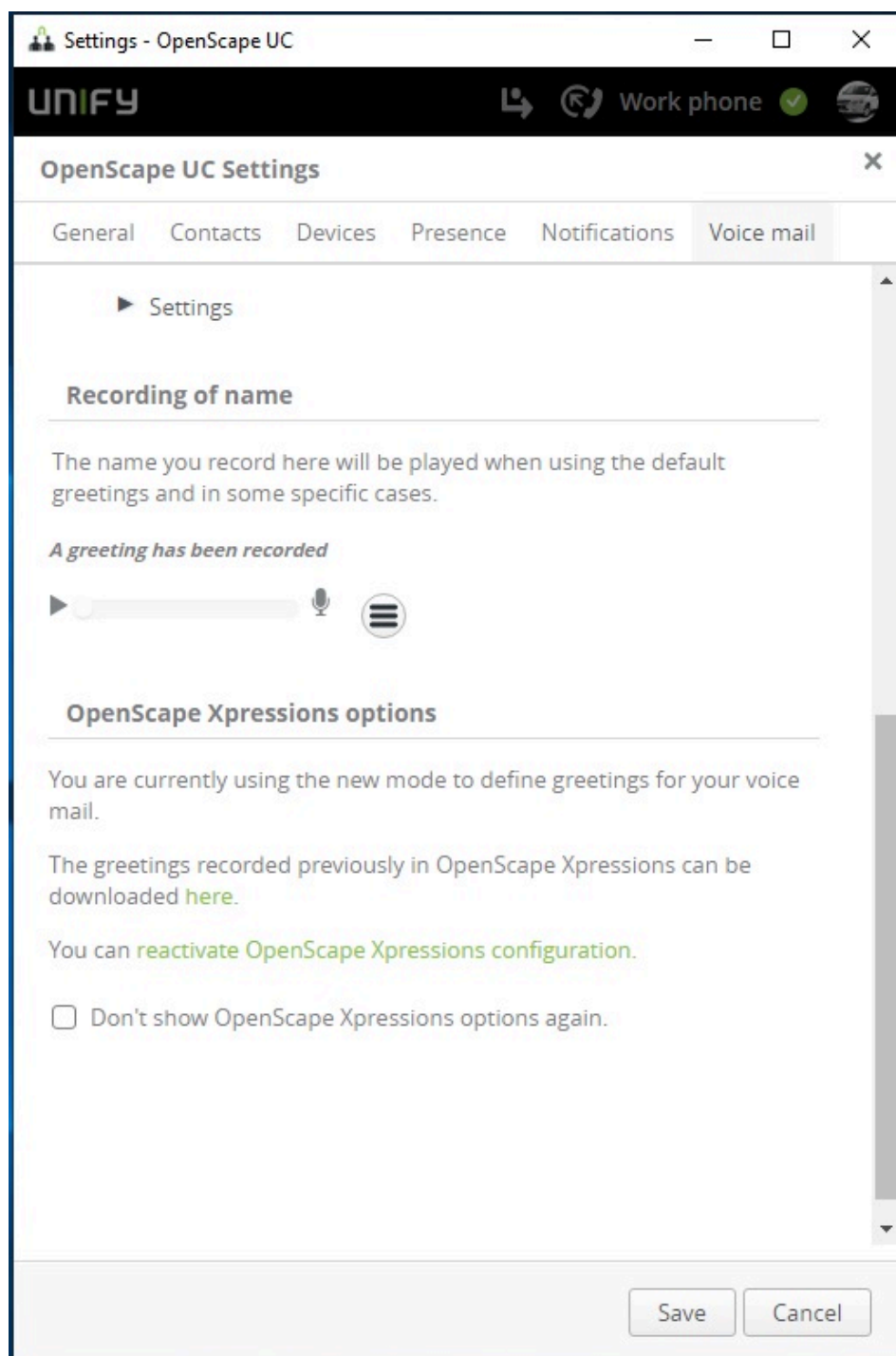
Upon selecting the new mode, a warning message comes up, and asks you to confirm the procedure.

When you confirm the change to the new mode, a backup of voice mail settings of OpenScape Xpressions Webassistant will start and the new greetings interface will be available (UCMODE=N).

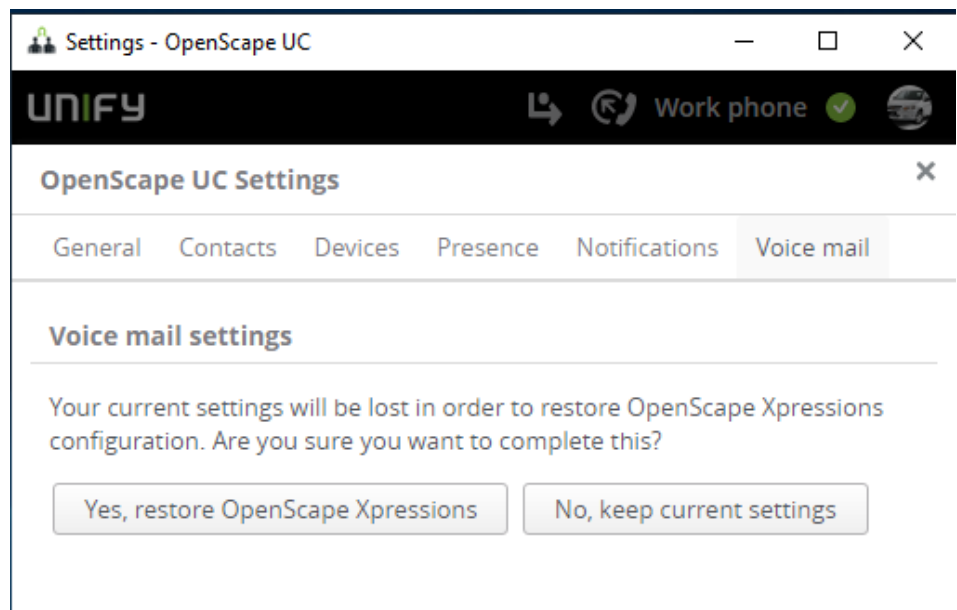
In the new greetings interface, there is a link to download a backup of previously recorded greetings (only personal greetings are backed up - system administrator greetings will not be in the backup file).

In the end, you have the option to reactivate the OpenScape Xpressions Configuration or mark the checkbox Don't show OpenScape Xpressions option again.





If you decide to reactivate the OpenScape Xpressions configuration, a warning message is displayed to inform you that all greetings and configurations done using the new mode will be lost in order to restore user old configuration of OpenScape Xpressions WebAssistant.



If you select Yes, restore OpenScape Xpressions, the OpenScape Xpressions configuration is displayed once again and the new mode option will still be available (UCMODE=O).

If you decide to continue in the new mode and select the option Don't show OpenScape Xpressions option again after pressing the save button, the OpenScape Xpressions reactivation option and the backup of greeting download will not be displayed again (UCMODE=U)

NOTICE: Only Xpressions System Administrator can reactivate the OpenScape Xpressions option again using the Infotool.exe.

3.16.2.7 OpenScape Xpressions WebAssistant Mode only (UCMODE = X)

This option is the same of Default option (UCMODE=X) when the user does not have the UC_MODE entry in the Xpressions correl database it will be created with value "X" to maintain the backward compatibility.

3.16.2.8 Unauthorized Mode - Voice mail tab disabled (UCMODE = D)

This mode can be used when the OpenScape Xpressions Administrator wants to force all company members to use a standard greeting for Voice mail and wants to prevent users from changing this standard greeting.

For these users, the OpenScape Xpressions Administrator should set the UCMODE to D.

In this mode, Voice mail tab is hidden and no options will be displayed (OpenScape Xpressions or New Greetings mode as shown in the figure below:

The screenshot shows a web browser window titled "Settings - OpenScape UC". The interface has a dark header with the "UNIFY" logo and a "Work phone" status indicator with a green checkmark. Below the header is a tabbed interface with tabs for "General", "Contacts", "Devices", "Presence", and "Notifications". The "General" tab is selected. The main content area is titled "OpenScape UC Settings" and contains several sections: "Software version information" showing "OpenScape UC Web Client V9.4-0.18.0-1174" and "Fusion 1.8.7.0 (Build 108)", with links for "Software license agreement for OpenScape UC Application", "Third party software information", and "International license agreement for non-warranted programs"; "Online help" with a link to "View our online help manual" and "View online help"; and "Location" with a text input field labeled "Type the name of the country you live in" and a placeholder "Type in the country name here...". At the bottom right are "Save" and "Cancel" buttons.

3.16.3 Basic Instructions to use the New Voicemail settings

3.16.3.1 New Interface of Voice Mail Settings

Once you select the new mode link from the Voice mail tab mode you will be prompted with a warning message to confirm the procedure. Select Yes, activate the new mode to access the new greetings interface.

In this new greetings interface, you can see the following sections and select the greetings configuration options.

- Voicemail settings

In this section you can select on of the following radio buttons:

- Default greetings - This is the Xpressions default greeting, that is, the initial setting that will be checked by default for all users.
- Single greeting - This option applies to users that want to use only one greeting all the time.
- Vacation greeting - This option will also set one special greeting to be used during a user's vacations. In addition, this option will automatically set calls to be forwarded to voicemail.
- Business greetings - This option applies to users that want to have two different greetings: one for business periods and one for non-business periods.

- Recording of name

Record or upload the name that will be plated in your default greetings options or other specific cases.

- OpenScape Xpressions options

In this section you can configure settings related to the OpenScape Xpressions integration

- You can access and download a backup of previously recorded greetings by clicking the download here link.
- You have also the option to reactivate the OpenScape Xpressions Configuration
- Or mark the Don't show OpenScape Xpressions option again checkbox to stop displaying your older Xpressions options.

NOTICE: Only the personal greetings are backed up. System administrator greetings will not be in the backup files.

3.16.3.2 How to Record and Play on Phone

Record on Phone and Play on Phone options are available in the Voice mail tab via the Greeting options menu:

Step by Step

- 1) Navigate to Settings > Voice mail tab.
- 2) Click on the  button to open additional Greeting options
- 3) Click Record on phone to record a greeting or click on Play on phone to hear an existing audio. It is also possible to record by clicking on the microphone icon.

While recording a greeting on the phone, the text Recording on phone will appear in red color until the recording is completed. If you are recording via a headset, similarly a Recording on headset will appear in red color.

Just after you finish recording your greeting, a new indication new greeting has been recorded will appear in green color.

IMPORTANT: LOOPDETECTION must be enabled in OpenScape Xpressions IpApl protocol. For detailed information regarding Openscape Xpressions IpApl protocols

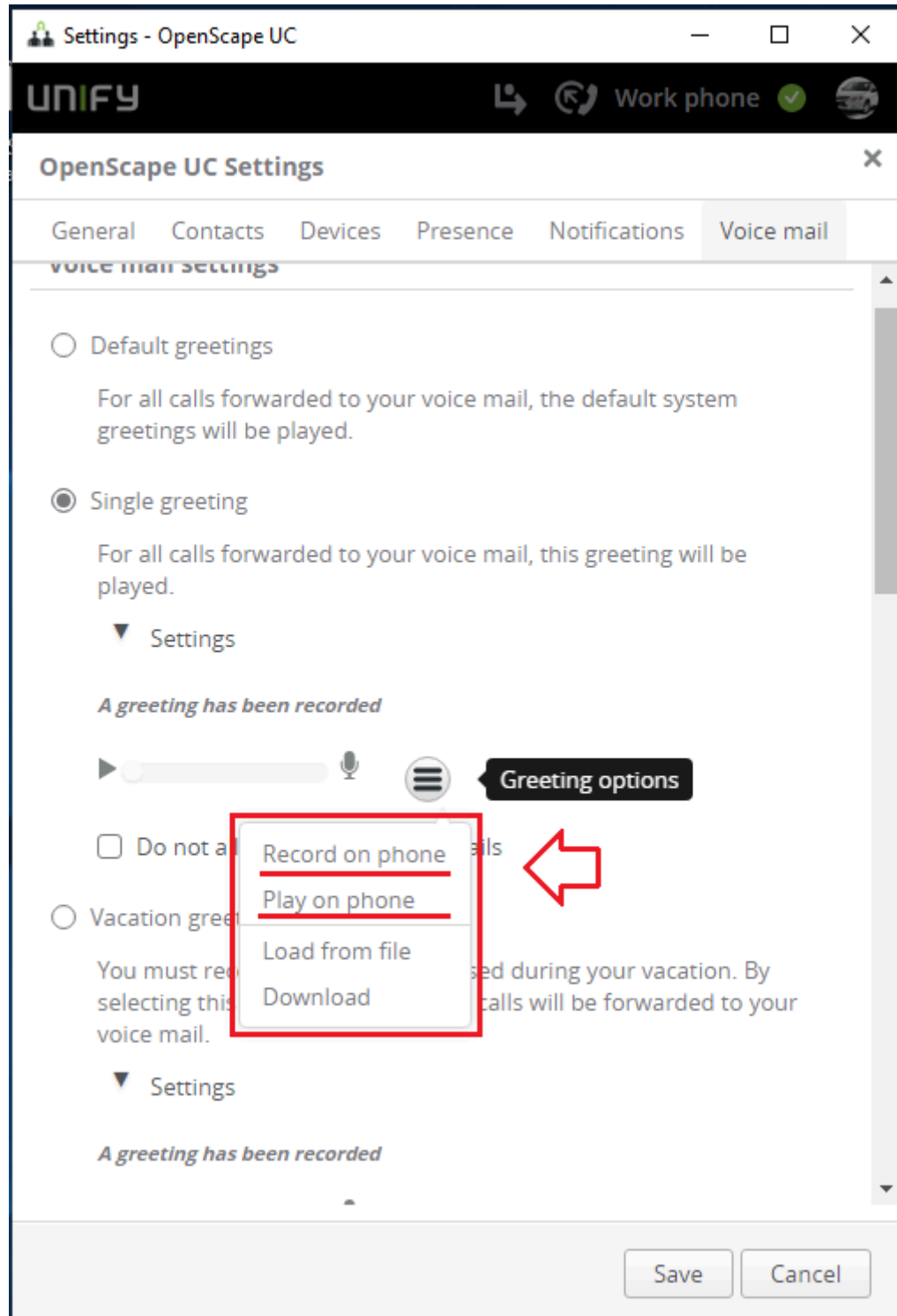
Features with individual Configuration

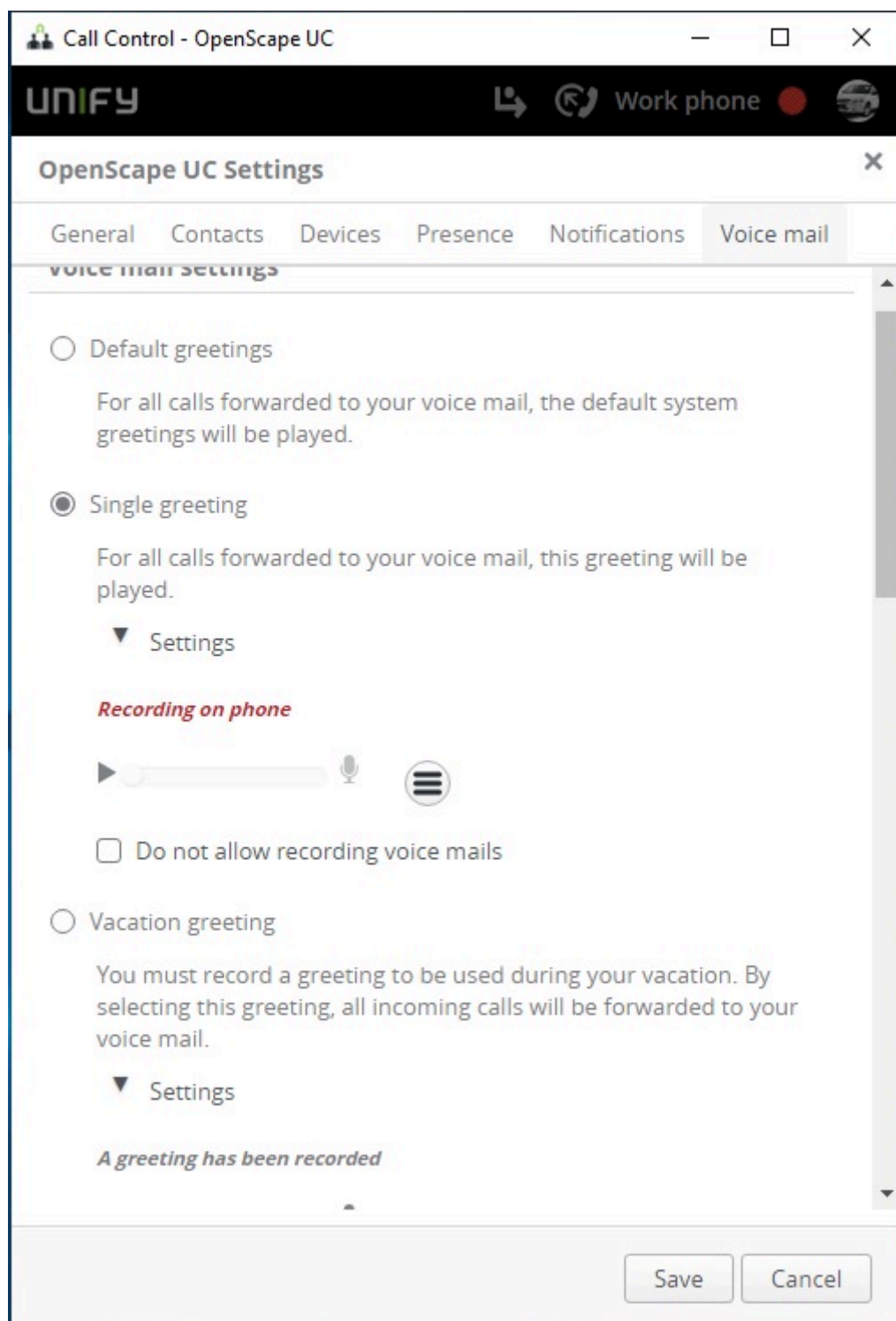
configuration please refer to OpenScape Xpressions V7,
Server Administration, Administrator Documentation.

4) Click Save to save your new greeting.

After clicking on Save, the indication A greeting has been recorded will appear in dark grey color. You can listen to your recording by clicking the play ► icon.

If there is no greeting available to play or download, the indication No greeting has been recorded will appear in light grey color.





NOTICE: The previously available options Play on the headset/Play on phone and Download will be disabled.

3.16.3.3 How to Upload and Download Greetings

Upload and download greetings options are available in the Voice mail tab via the Greeting options menu:

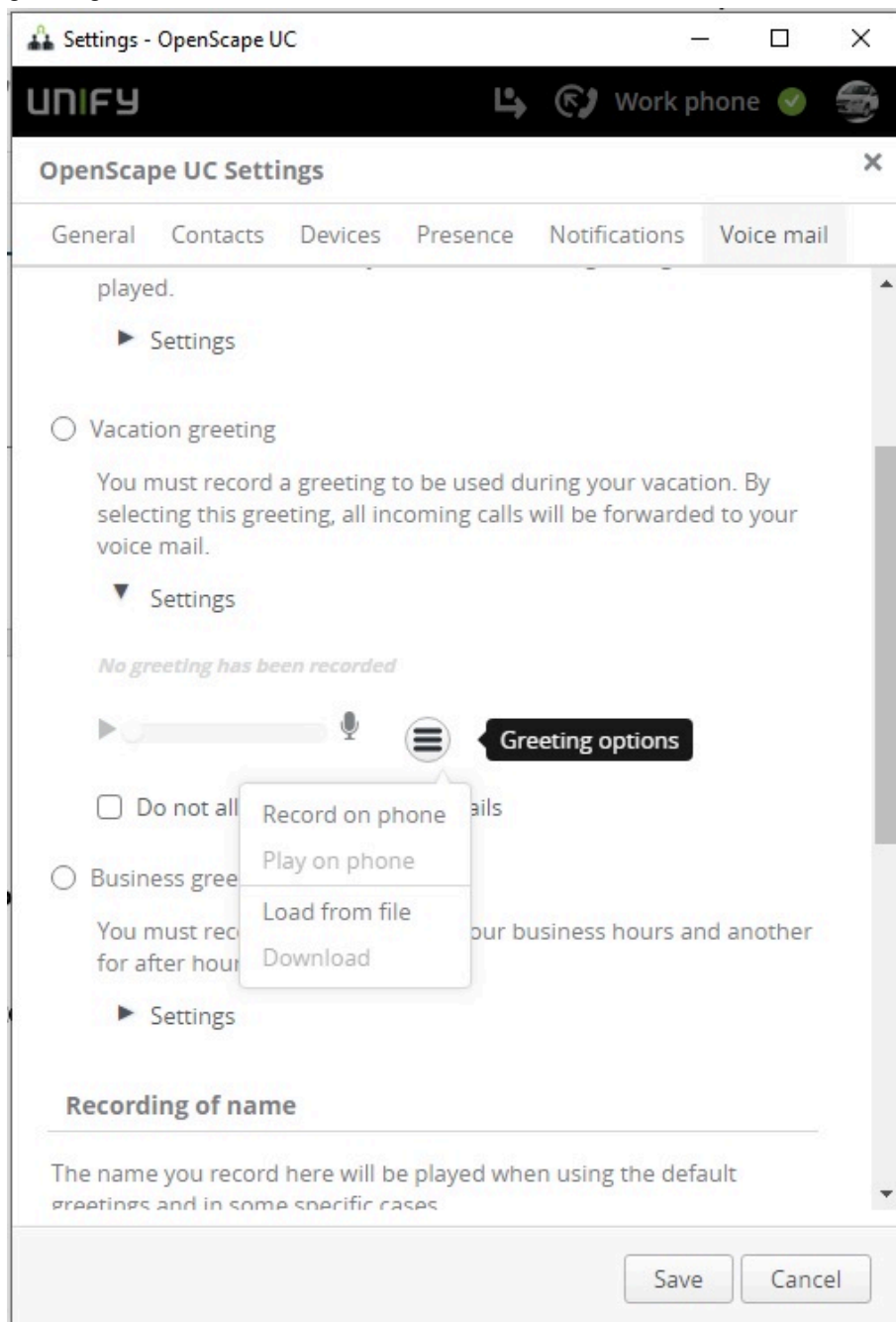
Step by Step

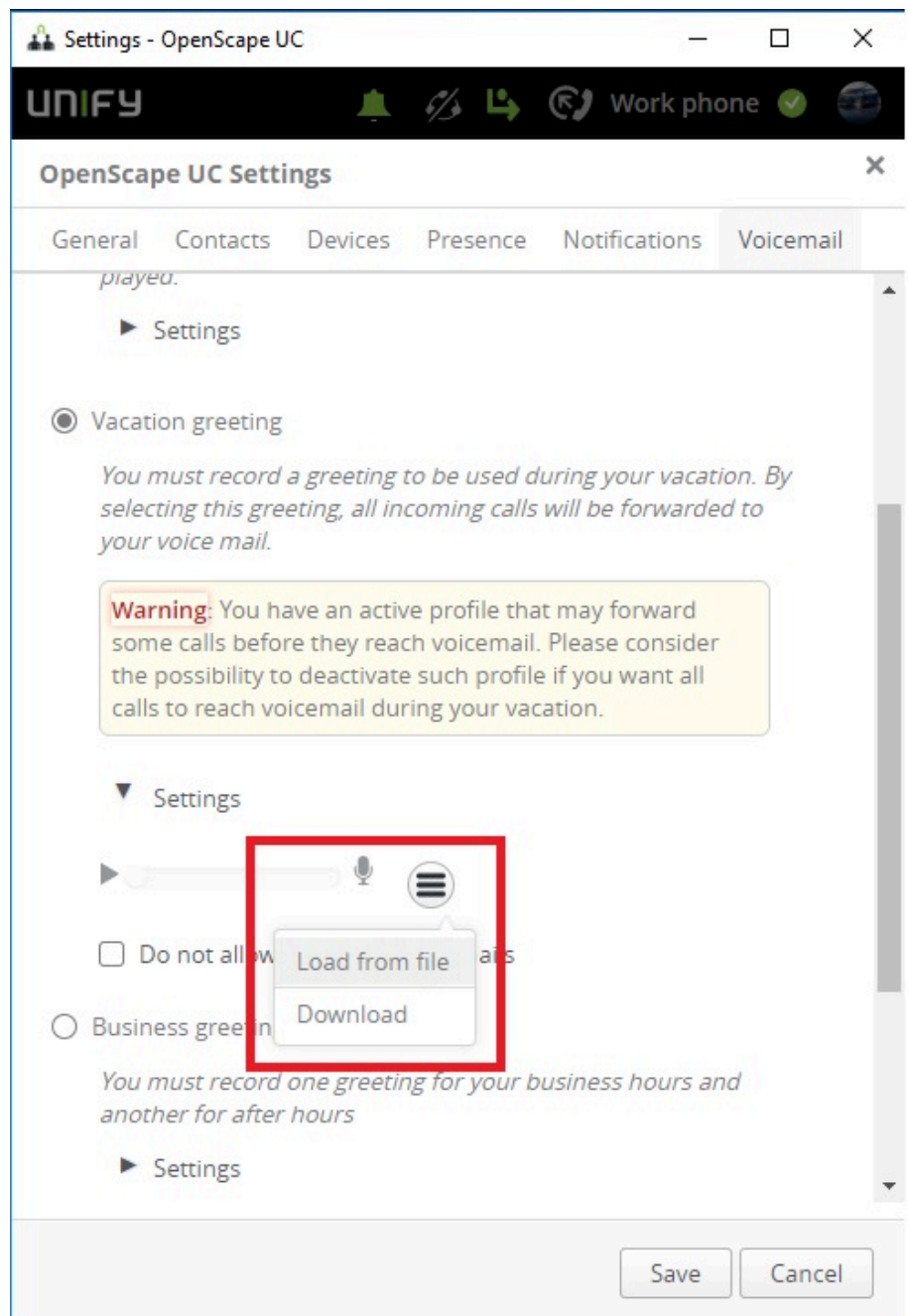
- 1) Navigate to Settings > Voice mail tab.
- 2) Click on the  button to open additional Greeting options
- 3) Click Upload from file to upload an audio file or click Download to download an existing audio greeting file.

IMPORTANT: Only .wav files are supported. The greeting file will also be downloaded as a .wav file.

NOTICE: Max. greeting length is 1 minute.

- 4) If you have uploaded an new audio file, click Save to save your new greeting.





3.16.3.4 How to Do not allow recording of voice mails

This option only applies for Single, Vacation and Business Greetings. By enabling this option you do not allow the recording of any voice mails.

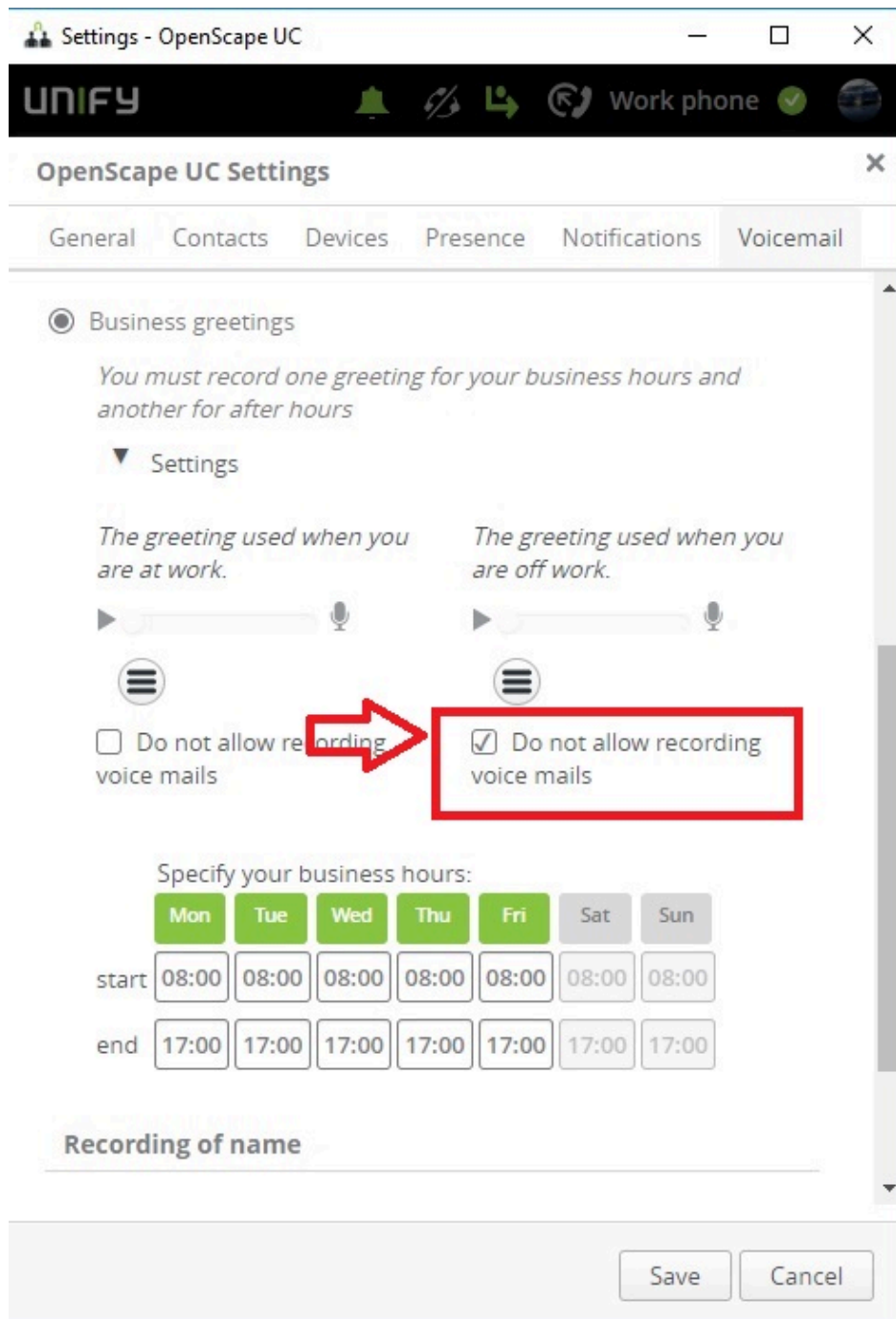
Prerequisites

- You have activated Single, Vacation or Business Greetings,

Step by Step

- 1) In the main OpenScope UC client interface navigate to Settings > Voicemail

- 2) In the Voicemail Settings section under your selected greetings option, check the Do not allow recording voice mails box.



Settings - OpenScape UC

UNIFY

OpenScape UC Settings

General Contacts Devices Presence Notifications Voicemail

☒ Business greetings

You must record one greeting for your business hours and another for after hours

Settings

The greeting used when you are at work.

The greeting used when you are off work.

☐ Do not allow recording voice mails

☒ Do not allow recording voice mails

Specify your business hours:

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
start	08:00	08:00	08:00	08:00	08:00	08:00	08:00
end	17:00	17:00	17:00	17:00	17:00	17:00	17:00

Recording of name

Save Cancel

NOTICE: You will get a prompt message: "This extension is not accepting messages".

3.16.3.5 How to Set Automatic Call Forward to Voice mail (only for Vacation greeting)

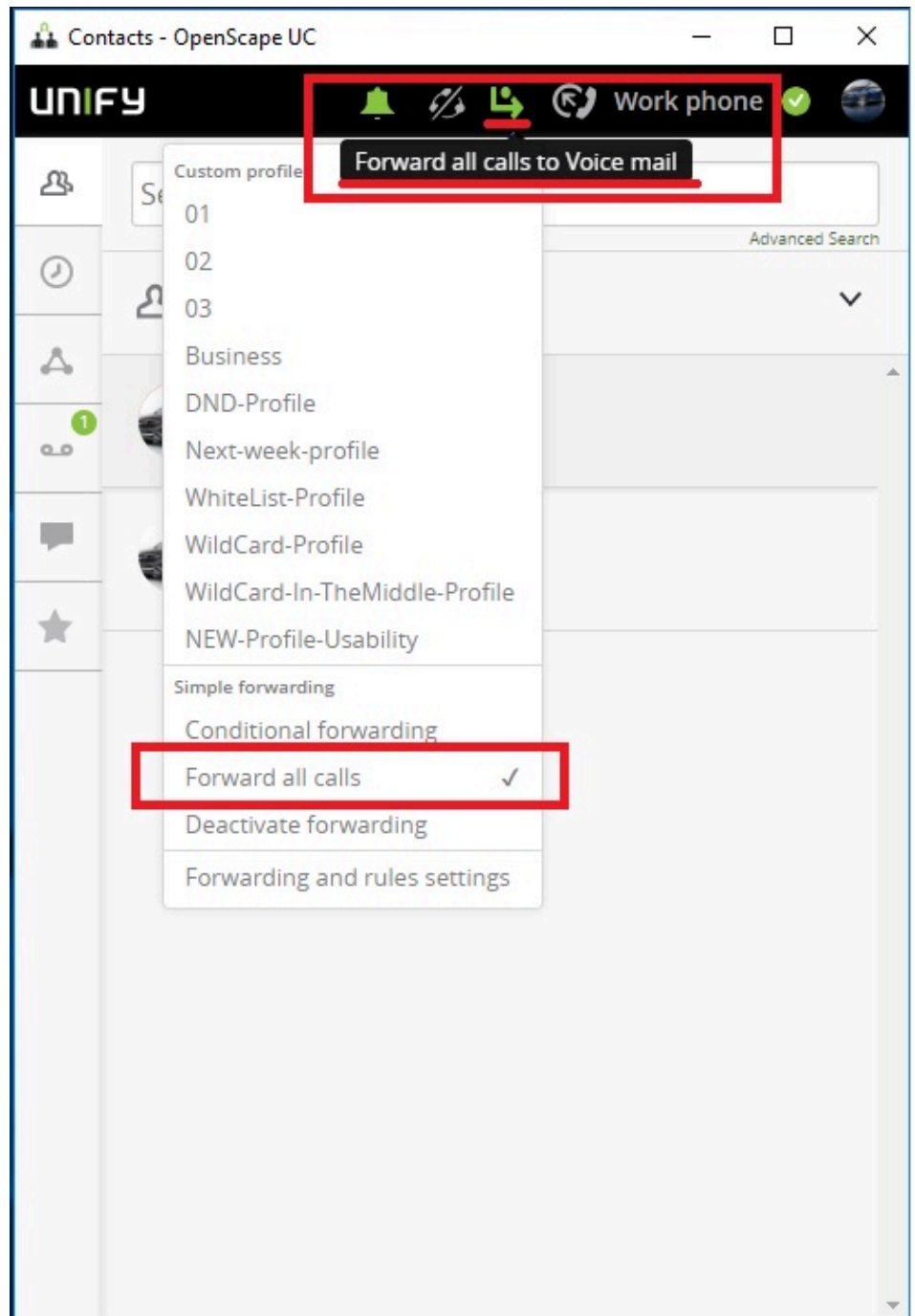
You can set an automatic call forwarding to your voicemail when Vacation greeting is activated. This option does not apply for another greeting selection.

Prerequisites

- You have activated Vacation greeting option.

Step by Step

- 1) In the main OpenScape UC client interface click on the  call forwarding icon
- 2) Select Forward all calls from the call forwarding options list.



IMPORTANT: This automatic call forward to voicemail will not be set if any previous call forward or rule is active.

NOTICE: To activate the call forward to voicemail again, the user should manually deactivate the previous call forward or rule first, then select another greeting (e.g. default greeting) and save; return to the Vacation greeting and save it again.

3.16.3.6 How to Set Business Greeting Time Profiles (only for Business greetings)

For Business Greeting setting, you have the option to use different greetings for working hours and after hours. You can select your weekdays and can specify your business hours for each day. The time profile can be configured in the new interface as following:

Prerequisites

- You have activated Business Greetings,

Step by Step

- 1) In the main OpenScape UC client interface navigate to Settings > Voicemail
- 2) In the Voicemail Settings section under Business greetings option:
 - a) Select your business days. under the Specify your business hours section.
 - b) Change manually the start and end hours for your selected business days.

3) Click Save to apply your changes.

Settings - OpenScape UC

UNIFY

Work phone

OpenScape UC Settings

General Contacts Devices Presence Notifications Voicemail

☒ Business greetings

You must record one greeting for your business hours and another for after hours

▼ Settings

The greeting used when you are at work.

The greeting used when you are off work.

☐ Do not allow recording voice mails

☒ Do not allow recording voice mails

Specify your business hours:

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
start	08:00	08:00	08:00	08:00	08:00	08:00	08:00
end	17:00	17:00	17:00	17:00	17:00	17:00	17:00

Recording of name

Save Cancel

3.16.4 Restrictions of the New UC greetings mode

- Upgraded scenarios from simplified, enhanced and system administrator greetings are not supported. Not supported configurations will be set to Default System configuration.
- No previous recorded greetings will be retrieved in the New Voice Mail Settings interface, except of the Personal Alternate greeting when it is used for all days of the week.
- There is no support of Simplified Default System greeting in the New mode. Only Enhanced Default System greeting is used in the New mode.

Features with individual Configuration

List of Useful Contacts

- There is no support of Internal/External/Busy greetings (External greeting will be used for all).
- Greetings backup zip file does not contain "Standard User greetings".
- Apple Safari browser is not supported by this feature.
- Microsoft Remote Desktop is not supported by this feature.
- Record or Play via headset is not supported by Microsoft Internet Explorer browser.
- Record or Play via headset is not supported by Desktop Integration Tool (DITOOL).
- Record or Play via headset is not supported by Fusion4Office CTI mode (DEFAULTPROVIDER=OSA-Provider).
- Record or Play via headset is not supported by Fusion4Office running on CITRIX environment.
- Record on headset is not supported using WebClient without secure connection (https).
- Greetings with length with more than 1 minute are not supported. 20~30 seconds greetings are recommended.
- Only .wav files are supported to use as greetings.
- Only English, German, French and Italian languages are supported.
- Disabling LOOPDETECTION in Xpressions IpApl is not supported because of Record on phone feature.

3.17 List of Useful Contacts

This feature allows UC administrators to create a common list of useful contacts for all users of the OpenScape UC system.

This list may contain up to 101 contacts that have in common a specific name for the department name field. This common name has to be defined by the administrator and it will be used as a search criteria to create the list of Useful Contacts.

Two parameters in the WebClientUI.cfg file are required for the activation of this feature:

- HandyContacts: the value of the department name defined by the UC administrator to be used in the search criteria for creating the list;
- HandyContactTitle: the name of this group of contacts to be presented in the user interface of UC Clients.

The List of Useful contacts will appear in the Contacts area of UC Clients, as well as in the Fusion Client Favorites panel.

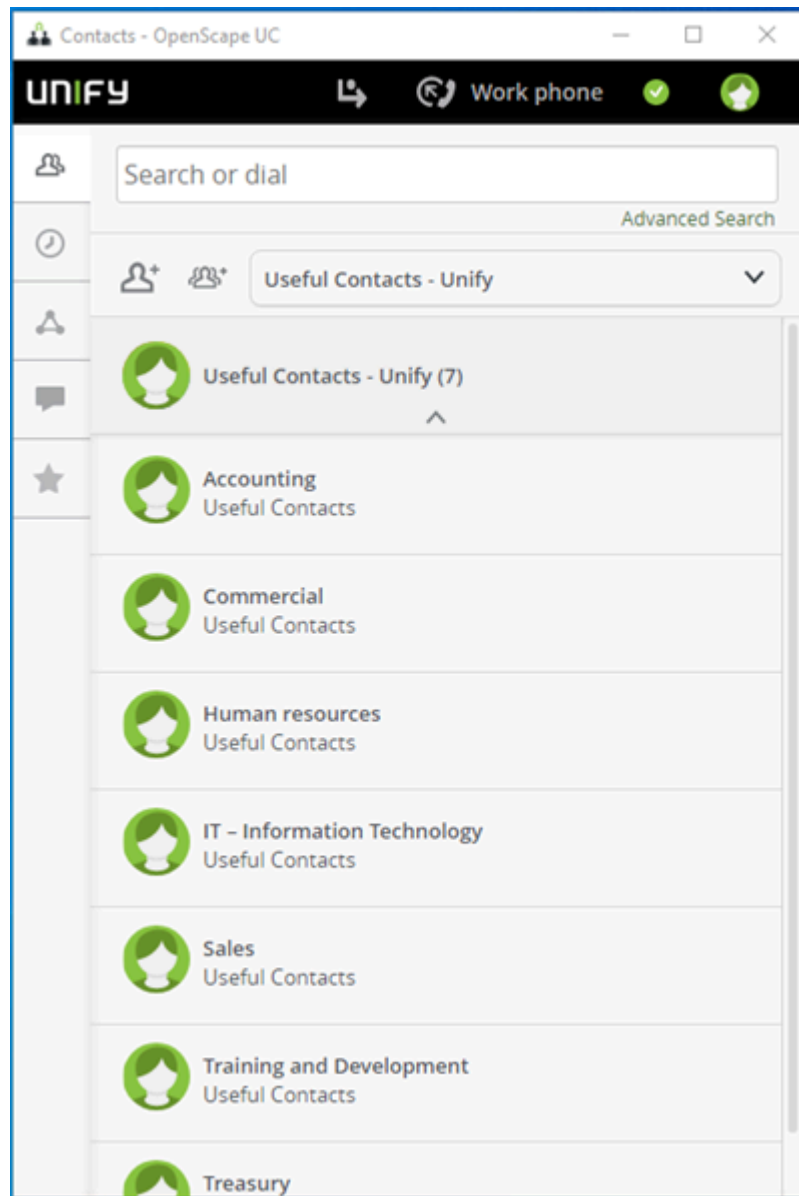


Figure 1: UC Client Contacts area

NOTICE: The WebClientUI.cfg file must be edited using the "UTF-8" encoding. The default encoding option ("1252 (ANSI - Latin I)") may cause the wrong display of characters in the WebClient UI.

Features with individual Configuration

Active Conference Notification

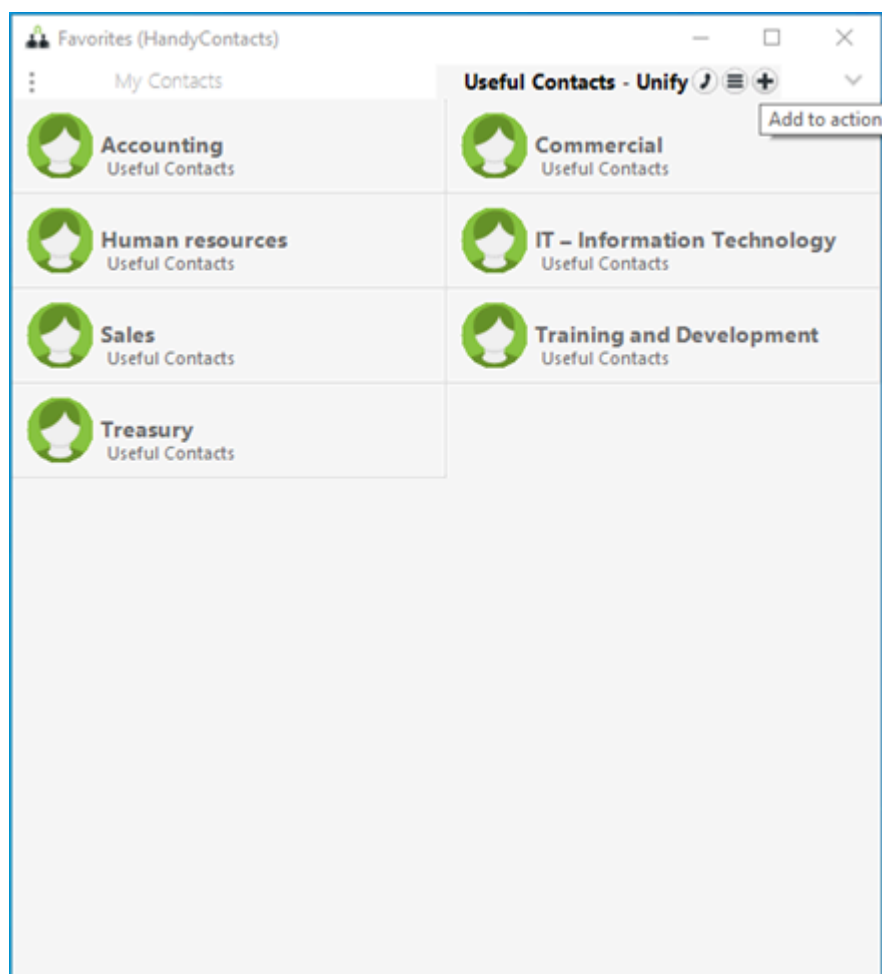


Figure 2: Fusion Client Favorites panel

HandyContacts - Backward Compatibility

The HandyContacts feature is only available for Fusion clients with version V2.1.19 or higher. For this feature to properly work, UC V11R4 must be used.

NOTICE: If UC V11R4 is used in combination with Fusion V1.8, then the List of Useful contacts will appear only in the extended view and not at all in the Favorites panel.

NOTICE: If UCV11 R3 is used in combination with Fusion V2.1.19, then the List of Useful contacts will not be available in the extended view, nor in the Favorites panel.

3.18 Active Conference Notification

The active conference notification allows users to be notified about all running conferences that they are invited to.

To enable the active conference notification, set the following key in the WebClient.CFG:

`showConferenceNotification = true`

3.19 Active Conference Tab and Avatars

Each conference will be displayed using a colored avatar.

To enable the colored conference avatar feature, set the following key in the WebClient.CFG:

`showConferenceNotification = true`

3.20 How to allow Softphones to automatically answer conference calls

To allow Softphones to automatically answer conference calls, set the following key in the WebClient.CFG:

`autoAnswerConferenceCall = true`

3.21 How to configure the Headset Service

The Headset Service module allows for controlling Jabra devices using Jabra SDK, Epos/Sennheiser devices, and Poly/Plantronics devices instead of the UC Desktop App HID native module.

To enable or disable the Headset Service, you need to set the headsetService configuration flag in the deployment.json file to the appropriate value. The default value of the flag is true ("headsetService" : true).

Epos/Sennheiser devices requirement:

To enable the headset integration for the UC Desktop App client, you must install the EPOS Connect software on your computer.

The binary files are located in:

<UCDesktopApp Installation folder>\headsetsvc

The log files are located in:

%LOCALAPPDATA%\Temp\UCDesktop\HeadsetService.log

3.22 How to configure the Password Reset Service

This service allows the user to request a password reset in case the password is forgotten or the account has been locked due to inactivity or to multiple failed login attempts.

To enable the Password Reset service, you need to configure the following parameters:

- **allowResetPassword** in the **WebClientUI.cfg** file

Path: /opt/siemens/HiPathCA/config/common/WebClientUI.cfg

Default value: false

If the **allowResetPassword** parameter is set to true, the user will be able to request a password reset in the login screen of the OpenScape Web Client or the Fusion for Office client.

- **Mail.Server** and **Mail.Sender** in the **JMailService.cfg** file

Path: /opt/siemens/HiPathCA/config/services/default/JMailService/JMailService.cfg

The **Mail.Server** and **Mail.Sender** parameters must be set according to the name of your mail server for outgoing messages.

Configuration example for the Fusion for Office client:

Mail.Server = exch.fusion6.net

Mail.Sender = administrator@fusion6.net

- **PeriodOfInactivity** in the **Config.xml** file

Path: /opt/siemens/common/conf/PassphrasePolicyConfig.xml

Default value: 90 days

The **PeriodOfInactivity** parameter is related to the **LockoutTime** parameter in the **Config.xml** file. The **LockoutTime** is set in days and represents the maximum period until the account is locked due to inactivity.

- **MaximumFailedAttempts** in the **PassphrasePolicyConfig.xml** file

Path: /opt/siemens/common/conf/PassphrasePolicyConfig.xml

Default value: 5

The **MaximumFailedAttempts** parameter represents the maximum failed password attempts allowed until the account gets locked.

The password reset URL is set in the **JMailService.cfg** file in one of the following ways:

- Add the URL via the **PasswordResetHost** parameter

PasswordResetHost = https://<host>:<port>

Example: PasswordResetHost = https://uc.test.net:8443

Path: /opt/siemens/HiPathCA/config/services/default/JMailService/JMailService.cfg

The **PasswordResetHost** parameter uses a specific public host link to reset the password.

- Assign a variable using the TelasWeb.cfg file

Example:

In the JMailService.cfg file, set the PasswordResetHost parameter:
PasswordResetHost = <?x \$UserEntryURL?>

In the TelasWeb.cfg file, set the UserEntryURL parameter: <?x set
UserEntryURL = "https://uc.test.net:8443" ?>

Path: /opt/siemens/HiPathCA/config/common/TelasWeb.cfg

After configuring the above parameters, restart the server for the changes to be applied.

3.23 How to configure the Password Expiration Notification Service

This service allows the user to be notified about the password expiration in the OpenScape Web Client UI or via an email sent to the email address associated with the user's account.

To enable the Password Expiration Notification service, you need to configure the following parameters:

- **PasswordNotification in the WebClientUI.cfg file**

Path: /opt/siemens/HiPathCA/config/common/WebClientUI.cfg

Default value: false

If the PasswordNotification parameter is set to true, the user will be notified about the password expiration.

- **Mail.Server and Mail.Sender in the JMailService.cfg file**

Path: /opt/siemens/HiPathCA/config/services/default/JMailService/
JMailService.cfg

The Mail.Server and Mail.Sender parameters must be set according to the name of your mail server for outgoing messages.

Configuration example for the Fusion for Office client:

Mail.Server = exch.fusion6.net

Mail.Sender = administrator@fusion6.net

- **Mail.PasswordExpiration in the JMailService.cfg**

Path: /opt/siemens/HiPathCA/config/services/default/JMailService/
JMailService.cfg

Default value: false

The Mail.PasswordExpiration parameter must be set to true to allow the user to receive an email notification about the password expiration.

Features with individual Configuration

How to enable the Whiteboard feature

- **MaximumAge in the PassphrasePolicyConfig.xml file**

Path: /opt/siemens/common/conf/PassphrasePolicyConfig.xml

Default value: 90 days (7776000000 milliseconds)

The **MaximumAge** parameter is set in milliseconds and represents the maximum period until the password expires. The expiration day is checked overnight for every user.

After configuring the above parameters, restart the server for the changes to be applied.

3.24 How to enable the Whiteboard feature

During an active conference, the participants can use the whiteboard feature to type notes, draw, or import images on a blank page.

UC users can use this feature if:

- A system administrator enables the **allowWhiteboardView** property in the WebClientUI.cfg file.
- The Whiteboard option is enabled in user's CMP profile.

Follow the steps below to enable this feature via the WebClientUI.cfg file:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

/opt/siemens/HiPathCA/config/common/WebClientUI.cfg

- 2) Set the value of the allowWhiteboardView property to true to enable the feature.

```
allowWhiteboardView = true
```

The default value is false.

- 3) Save the changes in the configuration file.

Follow the steps below to enable this feature via the CMP user profile:

- 1) In the CMP portal, navigate to Configuration > Unified Communications > Accounts > List. A list of all users is displayed.
- 2) Locate the desired user and click on it.
- 3) Open the **Profiles** tab.
- 4) Enable the **Whiteboard** option.

NOTICE: Changes to the CMP profile are only necessary for users who want to start the whiteboard during a conference call. Users without the Whiteboard option enabled in their profile can only use this feature if another conference attendee starts it during the conference call.

3.25 How to enable the Survey feature

Surveys can be distributed to users to get their opinion on specific topics.

UC users can use this feature if:

- A system administrator enables the **allowWhiteboardView** property in the WebClientUI.cfg file.
- The Whiteboard option is enabled in user's CMP profile.

Follow the steps below to enable this feature via the WebClientUI.cfg file:

- 1) Open the following configuration file with a text editor:
WebClientUI.cfg

You can find this file in the following folder of the application computer:
/opt/siemens/HiPathCA/config/common/WebClientUI.cfg

- 2) Set the value of the allowWhiteboardView property to true to enable the feature.

```
survey.enabled = true
```

The default value is false.

- 3) Save the changes in the configuration file.

Follow the steps below to enable this feature via the CMP user profile:

- 1) In the CMP portal, navigate to Configuration > Unified Communications > Accounts > List. A list of all users is displayed.
- 2) Locate the desired user and click on it.
- 3) Open the **Profiles** tab.
- 4) Enable the **Whiteboard** option.

NOTICE: Changes to the CMP profile are only necessary for users who want to distribute surveys. If the Survey option is not enabled in their profile, users can only participate in surveys started or distributed by others.

3.26 How to enable the Chat in Conference feature for UC users

During an active conference, the participants can use the chat feature to exchange messages, links or attachments.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:
WebClientUI.cfg

You can find this file in the following folder of the application computer:
/opt/siemens/HiPathCA/config/common/WebClientUI.cfg

- 2) Set the value of the allowChatView property to true to enable the feature.
allowChatView = true

The default value is false.

- 3) Save the changes in the configuration file.

3.27 How to enable the Chat in Conference feature for guest users

By default, guest users are not allowed to use the chat functionality during conference calls.

However, moderators can add guest users to a conference chat if the following configuration changes are performed:

Features with individual Configuration

How to enable audio sharing during screen share

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **allowConferenceChatWithGuests** property to true to enable the feature.

`allowConferenceChatWithGuests = true`

The default value is false.

- 3) Save the changes in the configuration file.

After configuring the above steps, a new option will be displayed for moderators to add guest participants to the chat.

Moderators must refresh the browser window or close the client and start it again to view the new option.

3.28 How to enable audio sharing during screen share

For an improved screen sharing experience, you can share your system's audio along with your screen.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **WebRTC.EnableVideoPresentation** property to true to enable this feature.

`WebRTC.EnableVideoPresentation = true`

The default value is false.

- 3) Save the changes in the configuration file.

3.29 How to enable the Hands Up feature

During an active conference, the participants can use the Hands Up feature to indicate they want to speak, without interrupting.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **allowHandsUpView** property to **true** to enable this feature.

`allowHandsUpView = true`

The default value is **false**.

- 3) Save the changes in the configuration file.

3.30 How to enable the My Notes feature

My Notes feature allows you to store notes, files and pictures for yourself, in a temporary chat repository. You can save to your notes space during a conference call or from the My Notes area on your UC client.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **allowMyOwnChatNotes** property to **true** to enable this feature.

`allowMyOwnChatNotes = true`

The default value is **false**.

- 3) Save the changes in the configuration file.

3.31 How to enable the integration between multiple features

OpenScape UC allows the integration between the following features in conference calls:

- Screen share
- Whiteboard
- Chat in a conference call
- My notes

Using the feature integration, it is possible to capture a picture of what is being presented via screen share or what is being displayed inside the whiteboard. You can then share the picture in the conference chat or save it to your notes space.

NOTICE: You must first enable each feature individually, before enabling the integration.

Follow the steps below to enable the integration between these features:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

Features with individual Configuration

How to enable the OpenScape Add-ins download option

2) Perform the following configuration changes:

- a) Set the value of the **allowTakePicture** property to **true** to enable users to capture a picture of what is being shared via screen share or what is being displayed inside the whiteboard.

`allowTakePicture = true`

The default value is **false**.

- b) Set the value of the **allowFWDChat** property to **true** to enable users to forward chat messages.

`allowFWDChat = true`

The default value is **false**.

NOTICE: The option to forward chat messages is not available on the Fusion for Office client. The **allowFWDChat** property must be set to **false** when **Fusion for Office** is used.

3) Save the changes in the configuration file.

3.32 How to enable the OpenScape Add-ins download option

OpenScape Add-ins is an integration between OpenScape UC and Microsoft Outlook. It extends Microsoft Outlook with features provided by OpenScape UC.

Follow the steps below to enable the OpenScape Add-ins download option:

1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- ### 2) Set the value of the **enableOpenScapeAddInsDownload** property to **true** to enable this feature.

`enableOpenScapeAddInsDownload = true`

The default value is **false**.

3) Save the changes in the configuration file.

3.33 How to enable the OpenScape Headset integration download option

OpenScape Headset integration allows you to control UC calls directly from your headset.

Follow the steps below to enable the OpenScape Headset integration download option:

1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **WebRTC.HeadsetIntegration** property to **false**.
`WebRTC.HeadsetIntegration = false`

The default value is **false**.

NOTICE: If set to `true`, the WebClient will attempt to use the headset integration via Headset Integration application.

- 3) Save the changes in the configuration file.

3.34 How to enable the Video Effects feature

You can use video effects to change your background in video calls or conferences or when you are idle.

The following video effects are available: Blur, Office, Room, Shelf, Painting, Company.

Follow the steps below to enable the use of video effects:

- 1) Open the following configuration file with a text editor:
`WebClientUI.cfg`

You can find this file in the following folder of the application computer:
`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the following properties to the appropriate value, as described below:
 - a) Set the value of the **videoEffects.enableBlur** property to **true** to make the Blur effect available for users in **Settings > Audio/Video** area of their UC client.

`videoEffects.enableBlur = true`

The default value is **false**.

- b) Set the value of the **videoEffects.background** property to **true** to allow users to replace their background with an image from the **Settings > Audio/Video** area of their UC client.

`videoEffects.background = true`

The default value is **false**.

- c) Set the value of the **videoEffects.debug** property to **true** to increase the debug level displayed in WebClient UI traces for the video effect feature.

`videoEffects.debug = true`

The default value is **false**.

- d) Set the desired value for the **videoEffects.frameRate** property to specify the fixed frame rate to be used by the video effect segmentation algorithm.

`videoEffects.frameRate = 25`

The default value is **25**.

- 3) Save the changes in the configuration file.

3.35 How to enable the Call Quality feature

During an active call, the Call Quality feature allows participants to view statistics about the quality of the audio, video or screen sharing connection.

Additionally, if the Call Quality feature is enabled, at the end of an audio call, participants are prompted to rate their audio experience on a scale of 1 to 5 stars.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the following properties to the appropriate value, as described below:

- a) Set the value of the **qualityofservice.monitoring** property to **true** to allow call statistics to be included in the UC client and server logs.

`qualityofservice.monitoring = true`

The default value is **false**.

- b) Set the value of the **qualityofservice.showInterfaceElements** property to **true** to display the call quality indicator in the call control of the UC client and a warning message in case the quality of the connection is poor.

`qualityofservice.showInterfaceElements = true`

The default value is **false**.

NOTICE: For the Call Quality feature to work properly, it is mandatory to enable both the **qualityofservice.monitoring** and **qualityofservice.showInterfaceElements** properties.

- c) Set the value of the **qualityofservice.rating** property to **true** to allow users to rate the quality of the connection at the end of the call.

`qualityofservice.rating = true`

The default value is **false**.

Call rating is displayed based on the following metric:

- Every **x** calls that have a duration that exceeds **y** seconds, the user is prompted to rate the overall quality of the connection.
- The value of **x** is determined based on the **qualityofservice.callNumber** property. The default value is **10**.
- The value of **y** is determined based on the **qualityofservice.duration** property. The default value is **120**.

- d) Set the value of the **qualityofservice.verbose** property to **true** to include additional logs about call metrics.

`qualityofservice.verbose = true`

The default value is **false**.

- 3) Save the changes in the configuration file.

3.36 How to enable the new Call Forwarding for internal/external call originators feature

As an administrator, you can now enable the new call forwarding feature for your users and allow them to forward calls based on the call origin (internal or external). If this feature is enabled, a new option is available in the **Simple forwarding** tab: **Check to distinguish internal from external calls**.

Follow the steps below to enable the new feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **callForwarding.allowNewCFWIntExtMode** property to **true** to enable this feature.

`callForwarding.allowNewCFWIntExtMode = true`

The default value is **false**.

If **callForwarding.allowNewCFWIntExtMode** is set to **false**, the **Check to distinguish internal from external calls** option is not displayed in the **Simple forwarding** tab and it is not possible to set forwarding rules based on the call origin.

- 3) Save the changes in the configuration file.

NOTICE: For OpenScape 4000 subscribers, it is only possible to configure call forwarding for internal and external originators for the **Always forward** mechanism. For more information, please refer to [Enabling Call Forwarding for Internal and External Originators for OpenScape 4000 Subscribers](#) on page 137.

4 System Configuration

NOTICE: All information about Large Deployment apply likewise for Very Large Deployment except as otherwise described.

This chapter provides information about the following topics:

- [Configuration Requirements](#)
- [Overview of the Configuration Process](#)
- [Configuration Checklist](#)
- [Changing the Deployment Scenario](#)
- [Configuration Preparations](#)
- [General Configuration](#)
- [Configuring the Communications System Connection](#)
- [Configuring the One-number Service \(ONS\)](#)
- [Configuring the Conference Portal](#)
- [Configuring the Voice Portal](#)
- [Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019](#)
- [Synchronizing the MS Teams Presence with OpenScape UC](#)
- [Configuring the IBM Lotus Domino Connection](#)
- [Configuring the LDAP Directory Connection](#)
- [Configuring the Instant-Messaging Connection](#)
- [Configuring the Connection to OpenScape Xpressions](#)
- [Configuring the System Networking](#)

4.1 Configuration Requirements

The following technical requirements must have been met before you can start the OpenScape system configuration:

- [General configuration requirements](#)
- [Configuration requirements for OpenScape Voice](#)
- [Configuration requirements for OpenScape 4000](#)
- [Configuration requirements for the Microsoft Exchange connection](#)
- [Configuration Requirements for Microsoft Lync Connection](#)
- [Configuration requirements for the IBM Lotus Domino connection](#)
- [Configuration requirements for the LDAP connection](#)
- [Configuration requirements for Instant Messaging Connection](#)
- [Configuration requirements for the OpenScape Xpressions connection.](#)

The following sections describe these requirements in detail.

General configuration requirements

The following general requirements must have been met before you can start the OpenScape system configuration:

- All UC Application nodes of the desired deployment scenario have been fully installed.
- Operable network connections exist between the UC Application nodes.

- You know the logon data for the CMP user account with the following ID: **administrator@system** The password for this user ID was specified during the setup and is stored in the Response File.

Configuration requirements for OpenScape Voice

The following requirements must be complied with for using OpenScape Voice as communications system at OpenScape UC Application:

- OpenScape Voice has been installed and is operable in a version released for OpenScape UC Application.

The *OpenScape UC Application, Planning Guide* manual describes which versions have been released .

- OpenScape Voice must be so configured that phone numbers are transferred to the OpenScape Media Server in the E.164 format (Global Numbering Format, GNF).
- If national numbering plans are used in OpenScape Voice, the associated country code must be configured in every OpenScape Voice switch by means of the `Srx/Main/OwnCountryCode` parameter. Beyond that, a corresponding prefix access code must be created in OpenScape Voice for this country code.

NOTICE: OpenScape Voice resources must not be transferred to OpenScape UC Application until the `OwnCountryCode` parameter has been configured in OpenScape Voice. OpenScape Voice resources transferred to OpenScape UC Application before the `OwnCountryCode` configuration must be deleted from the OpenScape UC Application database.

Configuration requirements for OpenScape 4000

The following requirements must be complied with for using OpenScape 4000 as communications system at OpenScape UC Application:

- OpenScape 4000 has been installed and is operable in a version released for OpenScape UC Application.

The *OpenScape UC Application, Planning Guide* manual describes which versions have been released .

- OpenScape 4000 Assistant / Manager is installed and operable.
- The configuration management (CM) of OpenScape 4000 Assistant / Manager is active and synchronized with the OpenScape 4000 database.
- The IP address for CSTA has been configured for OpenScape 4000.

NOTICE: You find detailed CSTA information for OpenScape 4000 in the *OpenScape 4000 CSTA and Phone Services, Service Documentation* manual.

A connectivity adapter with the following settings has been added for OpenScape 4000:

- Individual PBX link number
- Individual PBX sub-application-number
- Offered Mode

- The following configuration parameters must be added or set to value 1.
 - E164_NUMBER_FORMAT
 - CSTA3_DELAY_SST_CALL_RESP
 - CSTA3_DELAY_DEFLECT_CALL_RESP
 - CSTA3_DELAY_DEVICE_DEFLECT_CALL_RESP
- OpenScape 4000 modification in case numbers with Presentation Restricted are involved in UC scenarios

Starting with CSTA HF V11 R1.42.4, the parameter PRESENTATION_RESTRICTED is set by default to ignore in the UC dedicated profile of the default CSTA Adapter .

An application with the following settings has been added for OpenScape 4000:

- Individual application name
- Unused TCP port
- License type: **No license**

Port 7001 must be opened for communication between UC and OpenScape 4000.

The following timer must be configured in OpenScape 4000 to enable using the UC Application feature Tell-me-When:

- For a German OpenScape 4000 system
AE- CTIME:artswu=cptime1,dgvproab=30;
- For an English OpenScape 4000 system
CHA- CTIME:typeswu=cp1,eccssupv=30;

NOTICE: Each HP4K Manager or HP4K Assistant can only be added to one CMP. This means if you have your HP4K ElementManager added to one CMP Server, you cannot add it to another one. This limitation includes HPUM as well with the CMP. To add a HP4K node [available button “Add HiPath4000”] at CMP you need to have pre-installed the extra add-on package from the DVD installation .iso at your CMP/Offboard

#. zypper in OpenScapeUC_4kaddons

At CMP you need to save only the HP4K Manager node and not the HP4Ks systems that this manager administrates. Once your HP4K Manager saved OK, the HP4Ks systems will populate as well [These newly added Nodes are initially marked as “Incomplete” in the Node List so you have to Edit them and apply the appropriate settings on them; IPs; Pwd; etc.]

In case you experience issues saving HiPath4000 Manager as node to CMP, check the following:

- restart all HP4K Manager needed processes @ HP4K Manager server

```
# bash
#. cs_ctrl stop
#. cs_control start
#. cs_control check
```

- check the HP4K Manager SdkConfig4444.xml file which stores the HP4K <-> CMP connection, in case your HP4K ElementManager has a connection with another CMP. If this is the case delete / rename it.

```
# cd /opt/cm/sad/UMP/config/
# mv SdkConfig4444.xml SdkConfig4444.xml.orig
```

- restart CMP / Offboard


```
# /etc/init.d/symphoniad restart
```
- try to resave your HP4K Manager node @ CMP

Configuration requirements for the Microsoft Exchange connection

If you wish to configure the Microsoft-Exchange connection, the following requirements must have been complied with.

The Microsoft Exchange server has been installed and is operable in a version released for OpenScape UC Application.

The *OpenScape UC Application, Planning Guide* manual describes which versions have been released .

A technical user account has been configured to which an e-mail address is assigned (mail-enabled). This user account must be an account in the respective Active Directory domain.

For connecting Microsoft Exchange Server 2013/ 2016 / 2019 (web-services-based):

- Impersonation by the technical user account must be configurable for the Exchange mailboxes of UC Application users.
- The remote power shell is installed on the computer system from which the impersonation shall be configured.

The application computer of OpenScape UC Application must have access to the SMTP server of the Microsoft Exchange server.

No SMTP proxy must be operated between the SMTP server of the Microsoft Exchange server and the application computer of OpenScape UC Application.

Such security devices are, for example, the ISA server (Internet Security & Acceleration Server) or the UrlScan tool.

You know the logon data for an Exchange user account that has administrative privileges for the Microsoft Exchange system.

This user account must have in particular the following administrative privileges for Microsoft Exchange 2013 / 2016/ 2019 to enable configuring the impersonation for the technical user account:

- Administrative privileges for the Microsoft Exchange server that was installed as client access server.
- Administrative privileges that allow adding and assigning roles and scopes.

An operable LAN connection exists between the application computer of OpenScape UC Application and the Microsoft Exchange server.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

In the following section you learn how to configure the Microsoft-Exchange connection:

- [Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019](#) on page 193.

Configuration Requirements for Microsoft Lync Connection

NOTICE: A project-specific release is required for connecting Microsoft Lync Server to OpenScape UC Application.

If you wish to configure the Microsoft Lync connection, the following requirements must have been complied with.

The Microsoft Office Communications Server or Microsoft Lync Server has been installed and is operable in a version released for OpenScape UC Application.

The *OpenScape UC Application, Planning Guide* manual describes which versions have been released .

OpenScape UC Application must have been installed with the option **MS-Office-Communication-Server-Integration**. The associated RPM package is then installed also.

You find details on this in the *OpenScape UC Application, Installation and Upgrade* manual.

The OpenScape UCMA Proxy Web Server is installed and operable.

You find details on this in the *OpenScape UC Application, Installation and Upgrade* manual.

An operable LAN connection exists between the application computer of OpenScape UC Application and the UCMA Proxy Web Server.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

If UCMA Proxy Web Server and Microsoft Office Communications Server / Microsoft Lync Server are installed on different computer systems, an operable LAN connection must exist between the UCMA Proxy Web Server and the Microsoft Office Communications Server / Microsoft Lync Server.

How to configure the Microsoft Lync connection is described in [Configuring the Skype for Business / Microsoft Lync Connection](#).

Configuration requirements for the IBM Lotus Domino connection

If you wish to configure the IBM Lotus Domino connection, the following requirements must have been complied with.

The IBM Lotus Domino server has been installed and is operable in a version released for OpenScape UC Application.

The *OpenScape UC Application, Planning Guide* manual describes which versions have been released .

IMPORTANT: The IBM Lotus Domino server must have been installed on a different computer system, independent from other OpenScape components.

The IBM Lotus Domino connector server is installed and operable on the computer system of OpenScape UC Application.

You find details on this in the *OpenScape UC Application, Installation and Upgrade* manual.

Between the computer system of OpenScape UC Application, the IBM Lotus Domino connector server and the IBM Lotus Domino groupware server exists an operable LAN connection.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

To enable an OpenScape user managing his/her IBM Lotus Notes contacts in the OpenScape clients, one of the following requirements must be complied with.

- The OpenScape user has been created in the IBM Lotus Domino server as roaming user. This is done by the IBM Lotus Notes administrator. A roaming user can access his/her individual IBM Lotus Notes client environment from different IBM Lotus Notes clients.
- The OpenScape user's private address book must have been stored on the IBM Lotus Domino server. The user needs to configure this private-address-book replication by himself/herself. User often have already configured this function for retrieving their data via the Lotus Notes web access.

How to configure the IBM Lotus Domino connection is described in [Configuring the IBM Lotus Domino Connection](#) on page 226.

Configuration requirements for the LDAP connection

If you wish to configure the LDAP connection, the following requirements must have been complied with.

An LDAP directory to be connected is installed and operable

You have the following information about the installation and configuration of the LDAP directory.

- IP address of the server on which the LDAP directory is installed.
- Logon data for a user account via which the LDAP directory can be accessed
- Information about the database structure, so that the database fields of the LDAP directory can later be assigned to the field names of OpenScape UC Application.

An operable LAN connection exists between the application computer of OpenScape UC Application and the computer system with the LDAP directory.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

How to configure the LDAP connection is described in [Configuring the LDAP Directory Connection](#) on page 260.

Configuration requirements for Instant Messaging Connection

If you wish to configure the instant-messaging connection, the following requirements must have been complied with.

The Openfire server has been installed and configured as far as necessary to make it operable.

You find details on this in the *OpenScape UC Application, Installation and Upgrade* manual.

IMPORTANT: When you install Small Deployment or Large Deployment for the first time we recommend to install the Openfire server on the application computer of OpenScape UC Application. You find details on this in the *OpenScape UC Application, Planning Guide* manual.

An operable LAN connection exists between the application computer of OpenScape UC Application and the Openfire server.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

Port 9090 must have been released in existing firewalls to allow remote access to the Openfire server via the web-based Openfire administration interface.

Port 9091 must have been released in existing firewalls to allow remote access to the Openfire server via the encrypted, web-based Openfire administration interface.

How to configure the IM connection is described in [Configuring the Instant-Messaging Connection](#) on page 266.

Configuration requirements for the OpenScape Xpressions connection

If you wish to configure the OpenScape Xpressions connection, the following requirements must have been complied with.

The OpenScape Xpressions server has been installed in version 5 SMR 4 or higher and is operable.

The OpenScape Xpressions server and OpenScape UC Application are connected to the same communications system.

The FI APL has been installed with the OpenScape Xpressions server and is operable.

The Web APL has been installed with the OpenScape Xpressions server and is operable.

The PhoneMail script has been configured in the XPR server and is operable.

You have the following information about configuring the PhoneMail script.

- The phone number for the Guest / Forward Access of the PhoneMail script.
- The phone number for the Direct Access of the PhoneMail script.

The OpenScape Xpressions server is connected with OpenScape Voice via an SIP trunk.

The OpenScape Xpressions server is connected to OpenScape 4000 via the IP APL and CorNet-IP.

An operable LAN connection exists between the application computer of OpenScape UC Application and the computer system with the OpenScape Xpressions server.

IMPORTANT: If the computer systems are interconnected via a WAN connection, timeouts may hamper the system communication or make it even impossible.

The Web Assistant has been installed with the OpenScape Xpressions server and is operable.

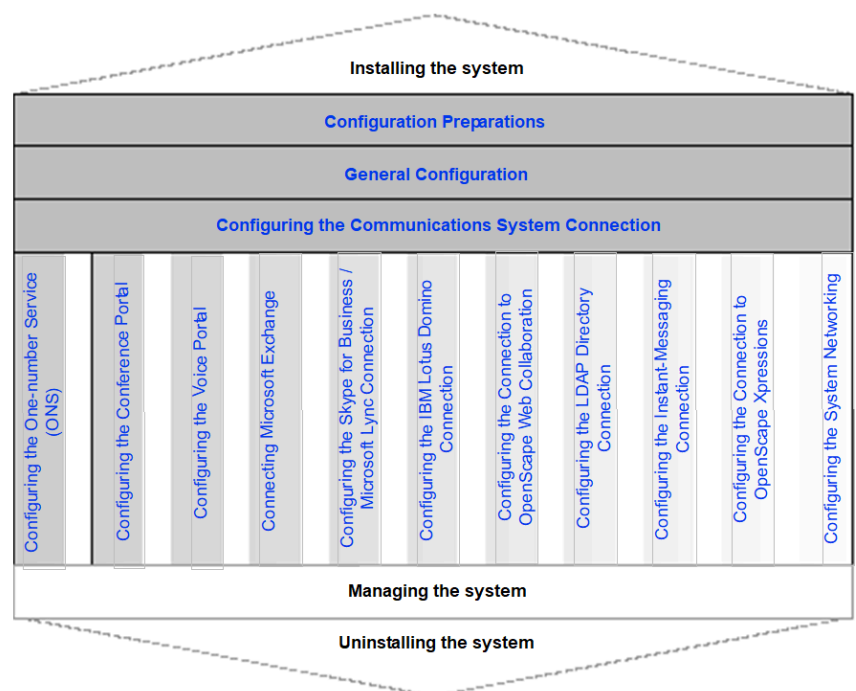
You know the login data for an XPR user account that possesses administrative privileges for the XPR server.

The start character (S) of the TTM phone number format must not be filtered out by the communications system or a gateway between OpenScape Xpressions server and OpenScape UC Application.

How to configure the OpenScape Xpressions connection is described in [Configuring the Connection to OpenScape Xpressions](#) on page 273.

4.2 Overview of the Configuration Process

The following figure provides an overview of the life time cycle of an UC Application system. The various system configuration areas are represented in detail.



The system configuration is divided into the following sections:

- [Configuration Preparations](#)

This section comprises first steps that you need to execute before the actual system configuration.

- [General Configuration](#)

This section comprises general configuration steps that you always need to execute and irrespectively of the features you may additionally configure at a later date.

- [Configuring the Communications System Connection](#)

This section comprises configuration steps that you need to execute for connecting a communications system. You need to execute the configuration steps for at least one of the described communications systems, irrespectively of the features you may additionally configure at a later date.

- Individual configuration of single features – e. g. the one-number service. Of the described features you need to configure only those that you want to use or for which you have purchased all required licenses.

NOTICE: Some of the described features are mutually exclusive. You find details about this in the respective configuration passage or in the *OpenScape UC Application Planning Guide*.

4.3 Configuration Checklist

IMPORTANT: In case of Very Large Deployment you need to execute most of the listed configuration steps for each cluster.

- 1) [Configuration Preparations](#)

[Sharing Protocol Ports in Firewall](#)

[Starting OpenScape UC Application](#)

- 2) [General Configuration](#)

For deployment scenarios with several front-end computers:

[Configuring the Load Balancer for Front-End Computers](#)

[Configuring the Load Balancer for Facade Servers](#)

Optional – For all deployment scenarios except for Integrated Deployment:

[Configuring IPsec](#)

[Activating Licenses](#)

[Configuring the Number of Connections for OpenScape Web Client](#)

If the OpenScape Web Client shall be opened via Internet Explorer:

[Configuring settings for the OpenScape Web Client in the Internet Explorer](#)

[Configuring the Presence Service](#)

[Creating a User Profile](#)

3) Configuring the Communications System Connection

For OpenScape Voice as communications system:

Connecting OpenScape Voice

- **Check:**

[Configuration requirements for OpenScape Voice](#)

[Checking OpenScape Voice Dependencies](#)

- **Optional – For all deployment scenarios except for Integrated Deployment:**

[Configuring a reduced OpenScape Voice Assistant](#)

- **For all deployment scenarios except for Integrated Deployment:**

[Configuring the OpenScape Voice System in the OpenScape Voice Assistant](#)

[Configuring the Synchronization of Business Group Data](#)

- **For deployment scenarios with a single Media Server entity:**

[Configuring the SIP Trunk in OpenScape Voice](#)

[Configuring the CSTA Link to OpenScape Voice](#)

[Configuring the Number of CSTA Sessions in OpenScape Voice](#)

[Configuring Office Codes](#)

[Configuring Prefixes](#)

- **For deployment scenarios with at least one independent Media Server computer system:**

[Configuring Packet Filters for Media Server Computer Systems](#)

- **For OpenScape 4000 as communications system:**

[Connecting an OpenScape 4000 System](#)

Check:

- [Configuration requirements for OpenScape 4000](#)
- [Configuring the SIP Trunk in OpenScape 4000](#)
- [Activating the Import / Export-API in OpenScape 4000 Assistant](#)

If you wish to connect several OpenScape 4000 systems to OpenScape UC Application using a OpenScape 4000 manager:

[Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager](#)

[Configuring a CSTA Connection to an individual OpenScape 4000 System](#)

For a mixed scenario of OpenScape 4000 and OpenScape Voice:

[Connecting various Communications Systems simultaneously \(mixed Scenario\)](#)

[Configuring Address Translation Contexts](#)

[Address Translation – Configuring St. Routing](#)

[Configuring the SIP Trunk in the OpenScape Media Server](#)

[Creating User Accounts](#)

4) [Configuring the One-number Service \(ONS\)](#)

[Configuring the ONS Number](#)

For OpenScape Voice as communications system:

[Activating the One-Number Service in OpenScape Voice](#)

For OpenScape Voice as communications system:

[Configuring the CTI Monitoring in OpenScape Voice](#)

For OpenScape Voice as communications system:

[Configuring an alternative Destination in OpenScape Voice](#)

[Configuring Device Settings](#)

5) Configuration of optional features

Optional: Configuring the Conference Portal

- [Configuring the Conference Portal Access](#)
- [Configuring a CTI Connection](#)
- [Configuring the Conference Component](#)
- [Configuring the Phone Number Normalization](#)
- **If you use video conferences of the conference portal by means of lifesize systems:**

[Activating RTCP for Video Conferences](#)

- **If you use several Media Servers operating in parallel:**

[Configuring the Conference Portal for Media Server Farm](#)

- **If you do not connect a groupware system:**

[Configuring the Conference Portal for Integrated Deployment with External Media Server for Video Conferences](#)

- **If you use video conferences of the conference portal:**

[Configuring Video Systems](#)

Optional: Configuring the Voice Portal

- [Configuring the User Access to the Voice Portal](#)
- **If you wish to use the OpenScape UC Application voice portal as voicemail system:**

[Configuring the Guest Access to the Voice Portal](#)

- **If you do not wish to use OpenScape Xpressions as voicemail system:**

[Configuring a Voicemail Number for Users](#)

- [Configuring the Phone Number Normalization](#)
- **If you use several Media Servers operating in parallel:**

[Configuring the Voice Portal for Media Server Farm](#)

- **If you use several Media Servers operating in parallel:**

[Configuring the Replication of Voice Portal Greetings](#)

Optional: Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019

- **Check:**

[Configuration requirements for the Microsoft Exchange connection](#)

- [Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019](#)

Check: [Configuration requirements for the Microsoft Exchange connection](#)

Optional: Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019

- **Check:** [Configuration requirements for the Microsoft Exchange connection](#)

[Configuring a technical User Account for Microsoft Exchange 2013 / 2016 / 2019](#)

[Configuring the Receive Connector for Microsoft Exchange 2013/ 2016 / 2019](#)

[Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019](#)

[Configuring the Groupware-Exchange Connector for Microsoft Exchange 2013 / 2016 / 2019](#)

[Creating User Assignments for Microsoft Exchange 2013/ 2016 / 2019](#)

[Importing User Assignments for Microsoft Exchange 2013/ 2016 / 2019](#)

[Configuring Access to Microsoft Outlook Contacts for Microsoft Exchange 2013/ 2016 / 2019](#)

[Configuring restricted Access to private Microsoft Exchange 2013/ 2016 / 2019 Contacts](#)

- *Optional:* [Configuring the IBM Lotus Domino Connection](#)

NOTICE: A project-specific release is required for connecting Microsoft Lync Server to OpenScape UC Application.

NOTICE: The connection to Microsoft Lync is not supported for Very Large Deployment.

- **Check:** [Configuration Requirements for Microsoft Lync Connection](#)
 - [Creating a Certificate Sign Request](#)
 - [Bind Certificate to Website](#)
 - [Exporting the Certificate for Client Use](#)
 - [Configuring SSL for UCMA Proxy Web Service](#)
 - [Configuring the Rights for the Use of the Certificate](#)
- **If the firewall of the UCMA proxy computer system integrated in Windows is activated:**
 - [Configuring a Firewall Rule](#)
 - [Configuring the Presence Service](#)
 - [Importing the Certificate to the OpenScape Application Computer](#)
 - [Creating User Assignments](#)
 - [Importing User Assignments](#)
 - [Configuring the IM Address for Users](#)
- **If you connect Microsoft Lync Server:**
 - [Activating additional Conference Features](#)

Optional: [Configuring the IBM Lotus Domino Connection](#)

Check: [Configuration requirements for the IBM Lotus Domino connection](#)

- [Creating a Linux User and Linux Group](#)
- [Configuring the Connector Server](#)
- [Stopping the Connector Server](#)
- [Creating a technical User Account](#)
- [Configuring Access Privileges for Mailboxes](#)

- [Configuring Access Privileges for Files](#)
- [Configuring the Groupware-Domino Connector](#)
- [Configuring the IBM Lotus Notes System Configuration](#)
- [Creating User Assignments](#)
- [Importing User Assignments](#)
- [Configuring Access to IBM Lotus Notes Contacts](#)
- **If OpenScape Conference Extension for Lotus Notes is to be used:**
[Configuring the IBM Lotus Domino Server for OpenScape Conference Extension](#)

Optional: [Configuring the LDAP Directory Connection](#)

- **Check:**
[Configuration requirements for the LDAP connection](#)
- [Configuring the Connection to the LDAP Directory](#)
- [Restarting the LDAP Connector Service](#)
- [Configuring the LDAP User Access](#)
- **If a Facade server is used:**
[Rebooting the Facade Server](#)

Optional: [Configuring the Instant-Messaging Connection](#)

Check:

[Configuration requirements for Instant Messaging Connection](#)

For all deployment scenarios except Very Large Deployment with several Openfire servers:

[Configuring the Openfire Server](#)

For Integrated Deployment:

[Creating Packet Filter Rules in OpenScape Voice](#)

[Configuring the IM Address for OpenScape Users](#)

[Creating and synchronizing Openfire User Accounts](#)

Optional: [Configuring the Connection to OpenScape Xpressions](#)

Check:

[Configuration requirements for the OpenScape Xpressions connection](#)

[Configuring Voicemail Numbers for Users](#)

[Assigning the Access Privilege](#)

[Configuring the Voice Portal Access](#)

[Installing the XPR Import Script](#)

[Configuring the XPR Import Script](#)

[Creating an XPR Import File](#)

[Importing an XPR Import File](#)

[Rebooting the XPR Server](#)

[Displaying PhoneMail Settings](#)

[Configuring XPR PhoneMail](#)

[Assigning a Privilege to XPR Users](#)

[Configuring the Web APL of OpenScape Xpressions](#)

[Changing UC Application User Profiles](#)

Optional: [Configuring the System Networking](#)

For Very Large Deployment with several Openfire servers:

[Configuring the Openfire Server](#)

[Configuring the Conference Portal](#)

[Configuring the Size of the JVM Heap](#)

4.4 Changing the Deployment Scenario

You can change a configured deployment scenario in the following manners.

- [Changing from Integrated Deployment to Small Deployment](#)
- [Changing from Small Deployment to Large Deployment](#)
- [Extending Large Deployment](#)

4.4.1 Changing from Integrated Deployment to Small Deployment

Only Professional Services & Solutions (PS & S) of Unify Software and Solutions GmbH & Co. KG may perform the change from Integrated Deployment to Small Deployment.

4.4.2 Changing from Small Deployment to Large Deployment

For this change of a deployment scenario you need to execute the following configuration steps.

NOTICE: The *OpenScape UC Application, Installation and Upgrade* manual describes how to install the necessary system nodes.

- 1) [Configuring additional OpenScape Media Servers](#)
- 2) [Configuring additional Front-End Servers](#)

Based on the Large Deployment redundancy concept we assume in the following description that you use Large Deployment with at least two OpenScape Media Servers and at least two front-end computers.

4.4.2.1 Configuring additional OpenScape Media Servers

You need to execute the following steps for the newly installed Media Server computers.

- 1) **Configuring the Communications System Connection**
[Configuring the SIP Trunk in the OpenScape Media Server](#)
- 2) **Configuring the Conference Portal**
[Configuring the Conference Portal for Media Server Farm](#)
- 3) **Configuring the Voice Portal**
 - a) [Configuring the Replication of Voice Portal Greetings](#)
 - b) [Configuring the Voice Portal for Media Server Farm](#)

4.4.2.2 Configuring additional Front-End Servers

You need to execute the following configuration step for the newly installed front-end computers.

[Configuring the Load Balancer for Front-End Computers](#)

4.4.3 Extending Large Deployment

If you have installed additional OpenScape Media Servers or front-end computers for Large Deployment you need to execute the following configuration steps depending on the changes.

NOTICE: The *OpenScape UC Application, Installation and Upgrade* manual describes how to install the necessary system nodes.

- 1) [Configuring additional OpenScape Media Servers](#)
- 2) [Configuring additional Front-End Servers](#)

4.4.3.1 Configuring additional OpenScape Media Servers

If you have installed additional OpenScape Media Servers for Large Deployment, you need to execute the following configuration steps.

- 1) **Configuring the Communications System Connection**
[Configuring the SIP Trunk in the OpenScape Media Server](#)
- 2) **Configuring the Conference Portal**
[Configuring the Conference Portal for Media Server Farm](#)
- 3) **Configuring the Voice Portal**
 - [Configuring the Voice Portal for Media Server Farm](#)
 - [Configuring the Replication of Voice Portal Greetings](#)

4.4.3.2 Configuring additional Front-End Servers

If you have installed additional front-end computers for Large Deployment, you need to execute the following configuration step.

[Configuring the Load Balancer for Front-End Computers](#)

4.5 Configuration Preparations

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

You need to execute the following steps before you can configure the OpenScape system.

- 1) [Sharing Protocol Ports in Firewall](#) on page 96
- 2) [Starting OpenScape UC Application](#) on page 96

These steps are described in detail in the following sections.

4.5.1 Sharing Protocol Ports in Firewall

For OpenScape UC Application to operate smoothly the OpenScape system components must be able to communicate via different protocol ports. If you use firewalls in the network infrastructure, you may have to expressly share these ports in there.

In the *OpenScape UC Application, Installation and Upgrade* manual you find a list with the port numbers that OpenScape UC Application uses.

4.5.2 Starting OpenScape UC Application

IMPORTANT: Be sure to have configured all required workarounds before initially starting OpenScape UC Application. Which workarounds are required is outlined in the current OpenScape UC Application Release Notes respectively. If you do not consider mandatory workarounds, problems may arise at the system start and the system setup may even become unusable.

Start the configuration

How to start OpenScape UC Application:

- 1) Execute the following command on all computer systems on which you have installed OpenScape UC Application components.

NOTICE: For Large Deployment, start the application computer prior to all other computer systems. This enables the other computer systems to access the OpenScape UC Application database when they are started at a later date.

After the application computer start wait for a minute until you start the front-end computer and Media Server computer in any sequence or simultaneously.

```
/etc/init.d/symphoniad start
```

OpenScape UC Application starts.

- 2) Execute the following command to put out the system startup log continuously.

- For Integrated Deployment:

```
tailf /log/osgi.log
```

- In all other deployment scenarios:

```
tailf /var/siemens/common/log/osgi.log
```

While the system starts, the system start log `osgi.log` should not log any errors.

After the following message in the system start-up log, all OpenScape UC Application services are up and running.

```
***** Starting all instances done. *****
```

Depending on the system configuration, it may take several minutes until all users configured in the system have been activated.

- 3) Open the following error log file after the OpenScape UC Application startup has finished.

- For Integrated Deployment:

```
/log/osgi.err
```

- In all other deployment scenarios:

```
/var/siemens/common/log/osgi.err
```

The error log file should not contain an error message.

You have now started OpenScape UC Application successfully.

The preparative configuration steps are complete.

4.6 General Configuration

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

The OpenScape UC Application configuration requires the following general configuration steps. You always need to execute these steps, no matter which OpenScape UC Application features you will use.

1) For Large Deployment:

[Configuring the Load Balancer for Front-End Computers](#)

2) [Configuring the Load Balancer for Facade Servers](#)

3) **Optional – For all deployment scenarios except for Integrated Deployment:**

[Configuring IPsec](#)

4) [Activating Licenses](#)

5) [Configuring the Number of Connections for OpenScape Web Client](#)

6) **If the OpenScape Web Client is to be opened in the Internet Explorer:**

[Configuring settings for the OpenScape Web Client in the Internet Explorer](#)

7) [Configuring the Presence Service](#)

8) [Creating a User Profile](#)

These steps are described in detail in the following sections.

4.6.1 Configuring the Load Balancer for Front-End Computers

NOTICE: You need to execute the configuration steps of this chapter only if you use several front-end computers operating in parallel.

If you use several front-end computers operating in parallel, a load balancer is required in the network. This load balancer serves the following purposes:

- Distributing the HTTP / HTTPS communication of the OpenScape Web Clients among the different front-end computers. A client must then communicate with the same front-end computer after the connection setup during the entire connect time.
- Providing a central address for the discovery requests of the OpenScape Desktop Clients¹.

By discovery requests the OpenScape Desktop Client¹ determines the IP addresses of the application computer, the front-end computer and the Media Server computer. Subsequently, the OpenScape Desktop Client¹ communicates with these computers directly.

- Performing TLS encryption and decryption for all OpenScape servers to relieve the servers from this task (TLS offloading).

Any data traffic between OpenScape clients and OpenScape servers must be routed via the load balancer to enable the balancer executing these tasks. Besides general routing the following requirements must be complied with:

- The load balancer must provide a shared proxy server in the client subnet for all available front-end computers. All requests by the OpenScape Web Clients to the front-end services must be distributed among the different front-end computers via this proxy server.

¹ OpenScape Fusion

- The load balancer must provide in the client subnet one proxy server for every application computer, front-end computer and Media Server computer of the server subnet. The TLS offloading is realized via these proxy servers.

NOTICE: All other servers – e. g. Facade server and Openfire server – are irrelevant for configuring the load balancer.

- The internal VLAN address of the load balancer must be configured in the UC Application computer systems as gateway for the client subnet.

For an example overview of the UC Application components that concern the load balancer, please refer to [Overview of the UC Application components that concern the load balancer](#) on page 834. The contained information serves as sample for the configuration steps described in this chapter. You must adjust in particular the represented IP addresses to your individual system environment.

The following configuration guide exemplifies how the described requirements can be implemented with the load balancer F5 BIG-IP 1600. How to implement the described requirements for other load balancer systems is outlined in the documentation of the load balancer system used.

Start the configuration

How to configure the load balancer based on the example F5 BIG-IP 1600:

- 1) Create a routing rule in the application computer, in the front-end computers and in the Media Server computers for making these computers send data for the client sub-net (*in the example: 10.4.0.0 / 16*) to the default gateway (*in the example: 10.1.252.170*).

This ensures the data traffic from the OpenScape servers to the OpenScape clients always being routed via the load balancer.

- 2) Reboot all OpenScape UC Application computer systems.
- 3) Configure the internal and external VLAN in the load balancer.

In doing so please keep in mind that the entire data traffic between OpenScape clients and UC Application servers may be routed via the load balancer only.

- 4) Create in the load balancer a shared address pool for all front-end computers.
 - a) Assign the addresses of front-end computer 1 and front-end computer 2 to this pool.
 - b) Configure port number 7789 for this pool. The OpenScape Web Client communicates via this port.
 - c) Configure the desired type of load balancing for this pool.

This pool is used to distribute the connection requests of the OpenScape Web Clients among the front-end computers.

- 5) Create an HTTP profile in the load balancer.
 - Select the **All** entry under **Redirect Rewrite** in this process.
 - Set the session timeout value to at least 15 minutes.

This profile is used for controlling the TLS offloading for OpenScape Web Client connections.

- 6) Create a virtual server in the load balancer for the created front-end computer pool (port 7789). In this process:
 - Select the **Host** option as **Destination-Type**.
 - Specify the address of the relevant proxy server under **Destination-Address**.
 - Select the relevant pool under **Default Pool**.
 - Configure port number **8443** under **Service Port**. The OpenScape Web Client communicates via this port.
 - Select the newly created HTTP profile under **HTTP Profile**.
 - Select the default profile **clientssl** under **SSL Profile (Client)**.
 - Verify that the **cookie** default profile is selected under **Default Persistence Profile**.
- 7) If you want to allow unsecured connections via port 7789 for the OpenScape Web Client also, configure another virtual server in the load balancer for the configured front-end computer pool (port 7789).
 - Select the **Host** option as **Destination-Type**.
 - Specify the address of the relevant proxy server under **Destination-Address**.
 - Select the relevant pool under **Default Pool**.
 - Configure port number **7789** under **Service Port**. The OpenScape Web Client communicates via this port.
 - Select the default profile **http-lan-optimized-caching** under **HTTP Profile**.
 - Verify that the **cookie** default profile is selected under **Default Persistence Profile**.
- 8) Import the SSL certificate to be used for TLS offloading in the load balancer.

NOTICE: How to configure a comprehensive certificate strategy for the OpenScape system is described in [Configuring a Certificate Strategy](#) on page 646.

- 9) Assign the SSL certificate you have imported to the **clientssl** default profile. To resolve IP addresses, adjust the DNS configuration in such a way that each OpenScape UC Application computer system can be reached under a fully qualified domain name.
- 10) *Example of an application computer with two front-end and two Media Server computer systems:*

openscapebe.company.com	10.4.255.212
openscapefe1.company.com	10.4.252.161
openscapefe2.company.com	10.4.252.165
openscapems1.company.com	10.4.252.20
openscapems2.company.com	10.4.252.37

- 11) Furthermore, add in the DNS configuration another entry for the fully qualified domain name under which the virtual server shall be reachable for the pool of all configured front-end computers. (Compare step 6).

Example:

openscape.company.com	10.4.255.211

- 12) Add in the `system.xml` file an NAT mapping entry of the following format for each UC Application node.

```
<NATMappingTable>
  <Entry hostExternal ="< FQDN of the relevant node >"
    tenantID ="< FQDN of the front-end computer pool>"/>

</NATMappingTable>
```

In doing so, use:

- The node-individual fully qualified domain name you configured in step 10 for the `hostExternal` parameter.
- The fully qualified domain name you configured in step 11 for all `tenantID` parameters.

You find the `system.xml` file in the following directory on the application computer:

`<Osc-Install2>/common/conf/`

Example of an application computer with two front-end and two Media Server computer systems:

```
<Node displayname="Backend" guid="72ababd8-e065-4ba5-b5b1-c8ed32ccf5b0"
host="athol60" jGroupsPort="7800"
serviceContainer="true" type="BACKEND">
  <NATMappingTable>
    <Entry hostExternal="openscapebe.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
<Node displayname="FE Server 1" guid="59aac72a-fedf-4977-9a57-9afd7957bf45"
host="athol61" jGroupsPort="7800"
serviceContainer="true" type="FRONTEND">
  <NATMappingTable>
    <Entry hostExternal="openscapfe1.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
<Node displayname="FE Server 2"
guid="5f92643f-7cda-43b1-a64b-5e0e87f7d502"
host="athol65" jGroupsPort="7800"
serviceContainer="true" type="FRONTEND">
  <NATMappingTable>
```

² `<Osc-Install>` is the setup directory of OpenScope UC Application: `/opt/siemens/` respectively `/enterprise/`

```

        <Entry hostExternal="openscapefe2.company.com"
tenantID="openscape.company.com"/>
    </NATMappingTable>
</Node>
<Node displayName="MS 1"
guid="2f2105fe-3aa4-410d-9bd9-0dcb6a1c0a26"
host="atho37" jGroupsPort="7800"
serviceContainer="true" type="MEDIASERVER">
    <NATMappingTable>
        <Entry hostExternal="openscapems1.company.com"
tenantID="openscape.company.com"/>
    </NATMappingTable>
</Node>
<Node displayName="MS 2"
guid="d4ecaa73-8a78-4f3c-9262-783c666faa8a"
host="atho20" jGroupsPort="7800"
serviceContainer="true" type="MEDIASERVER">
    <NATMappingTable>
        <Entry hostExternal="openscapems2.company.com"
tenantID="openscape.company.com"/>
    </NATMappingTable></Node>

```

- 13) Reboot all OpenScape UC Application computer systems so that the `system.xml` file is replicated on all computer systems.
- 14) Configure in the OpenScape Desktop Client under **OpenScape Web Client host address** the address you added to the DNS configuration in step 11.
 - For encrypted communication with the host:
https://openscape.company.com:8443
 - For unencrypted communication with the host:
https://openscape.company.com:7789

NOTICE: You need to have created the virtual server in step 7 for the OpenScape Desktop Client to communicate unencrypted with the host.

How to configure **OpenScape Web Client host address** in the OpenScape Desktop Client describes the *OpenScape UC Application, OpenScape Desktop Client, Installation and Administration* manual.

- 15) Configure in the property file `properties.ini` of the Facade server for the `serverName` setting the fully qualified host name you added to the DNS configuration in step 11.

You find the property file in the following folder of the computer system on which the Facade server is installed.

`/usr/local/facade/conf/<installation directory of the Tomcat server>`

4.6.2 Configuring the Load Balancer for Facade Servers

NOTICE: You need to execute the configuration steps of this chapter only if you use several Facade servers.

To increase the number of simultaneously supported OpenScape Mobile Clients or to operate several Facade servers in an N+1 redundancy, you can configure several Facade servers.

In this case a load balancer is required in the network. This load balancer serves the following purposes:

- Distributing the HTTPS communication of the OpenScape Mobile Clients among the available Facade servers. In this process, a client must communicate with the same Facade server during the entire connection time after the connection setup.
- If desired: Performing the TLS encryption and decryption to relieve the Facade server from this task (TLS-Off-Loading)..

Configure the load balancer used in a similar manner as described in [Configuring the Load Balancer for Front-End Computers](#) on page 98. In doing so please heed the following points:

- The load balancer should distribute inbound HTTPS communication of the OpenScape Mobile Client between the available Facade servers applying the Round-Robin procedure.
- Configure the persistence based on the client IP address. Persistence based on client port, SSL-ID or Cookie is insufficient for the OpenScape Mobile Client communication.
- Configure TLS-Off-Loading if desired.

4.6.3 Configuring IPsec

NOTICE: You can execute the configuration steps of this chapter if you do not use Integrated Deployment.

The different components of an OpenScape system partly exchange security-relevant information – for example SIP access information between OpenScape UC Application and OpenScape Voice. We therefore recommend to operate all components of an OpenScape system in a shared, secured network.

If your network environment does not allow such a solution, we recommend to configure secured communication channels between the different OpenScape systems. You can provide such secured communication channels by the IPsec protocol, for example.

How to configure IPsec for securing the communication between the OpenScape systems is outlined in [IPsec Configuration](#) on page 691.

4.6.4 Activating Licenses

The legal use of the OpenScape system features requires the corresponding product licenses. You need to activate such licenses in the CMP.

OpenScape licenses can be activated by one of the following two methods:

- Online with license activation code (LAC)
- Offline with license file

You find detailed information about the license management in the CMP in the *OpenScape Common Management Platform, Administrator Documentation* manual.

Start the configuration

How to activate OpenScape licenses, for example offline with a license file:

- 1) Click on the **Licenses** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Management > Information**.

The workspace displays the license information.

- 3) Click on **Offline Activation**.

The dialog for activating a license file opens.

- 4) Click on **Browse** next to the **License file** field and navigate to the storage location of the license file you have received with the OpenScape product.
- 5) Click the **Activate** button.

The license management verifies the signature of the license file against the system server's MAC address (Locking ID). If the verification is successful, the data are transferred from the file and the licenses are displayed in the CMP with the associated information.

You have now activated the OpenScape licenses offline with a license file.

4.6.5 Configuring the Number of Connections for OpenScape Web Client

NOTICE: You need to execute the following steps on all user computer systems from which the OpenScape Web Client is invoked or on which the OpenScape Desktop Client WE is installed.

The Internet Explorer limits the number of connections that can be set up to the same web server simultaneously. The such restricted number of connections is in most cases not sufficient for making full use of the OpenScape Web Client.

We recommend to step up the number of connections used to at least value 16.

Increasing the limited number of connections on the OpenScape users' computer systems depends on the Internet Explorer version used.

Internet Explorer 7

Enter in the following registry value the number of connections that may be simultaneously set up with the same web server:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Internet Settings\ MaxConnections

Internet Explorer 8

Create one of the following new DWORD registry values in the registry and specify therein the number of connections that may be simultaneously set up with the same web server:

- For OpenScape Web Client users
`KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\ FEATURE_MAXCONNECTIONSPERSERVER\iexplorer.exe`
- For OpenScape Desktop Client WE users
`KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\ FEATURE_MAXCONNECTIONSPERSERVER\Siemens.OpenScape.exe`

4.6.6 Configuring settings for the OpenScape Web Client in the Internet Explorer

NOTICE: The following step must be made for all user computer systems from which the OpenScape Web Client is to be called via the Internet Explorer. This is the case if a user employs at least one of the following OpenScape clients: OpenScape Desktop Client WE, OpenScape Web Client, OpenScape Fusion for Microsoft Lync, OpenScape Fusion for IBM Notes, OpenScape Fusion for Office.

To enable using the OpenScape Web Client with the Internet Explorer, the following must be assigned to the **Trusted Sites** security zone of the Internet Explorer.

- For deployment scenarios without individual front-end computer the fully qualified domain name of the application computer.
- For all other deployment scenarios the fully qualified domain names of the front-end computer systems.

You can achieve this in two ways.

- Add the required domain names in the following place of the browser settings via a group policy. You find related details in the Microsoft product documentation.
- Add the required domain names in the following place of the browser settings:

Tools > Internet Options > Security > Trusted Sites > Sites > Advanced

4.6.7 Configure the contact display merging

For similar contacts one merged entry with all data is shown.

There will be a weight calculated for matching contacts:

The default threshold value for weight calculation is 0.7. Based on the following table, if the weight calculated is 0.7 or higher the contacts will be merged.

This threshold value can be adjusted via the parameter "ContactSearch.MergeThreshold" in the "WebClientServlet.cfg" file under

<Osc-Install>/HiPathCA/config/common.
ContactSearch.MergeThreshold = 0.7

Table 2: Match and mismatch weights for comparing contacts

Field	Match	Mismatch	Notes
First Name	0.3	-0.3	
Last Name	0.3	-0.3	
Phone	0.5		
E-Mail	0.5		
IM-Address	0.8	-0.2	
Presence-UID	1.0	-0.3	
Source-ID	1.0	-0.3	
Company	0.2	-0.1	
Department	0.2	-0.1	

Two or more contacts will be merged into one. After merging two contacts into one the original contacts are no longer taken into account for further comparisons or merges but only the already merged one. The merge result is taken into account for any future comparison, but for complexity reasons the comparison to contacts which were already compared to the original contact are NOT repeated.

- For all "non connection" fields (name, company, location, ...) If the same field is filled with different data in the source contacts, a directory priority will define which value will be added to the merged contact
- The merged contact will also contain an array of connection data regrouping all connection of each type (e.g. an array with 3 work phones, an array with 2 emails, ...)
 - The primary information (the one from the most prioritized directory) will be duplicated in the original field for compatibility purpose (the client will be able to ignore this fields through request filter)
- Directory order preference would be: Global, Groupware, LDAP
 - the directory order is configurable via the setting 'ContactSearch.ConnectorPrio' in the file WebClientServlet.cfg under

<Osc-Install>/HiPathCA/config/common

Example:

#first is highest prio, last lowest prio

ContactSearch.ConnectorPrio = svc-globalcontactlist,
VdGwService, svc-ldapconnector, svc-contactlist

For the changes to take effect a Web Client restart is necessary.

³ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

⁴ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

4.6.8 Configuring the Presence Service

You need to perform various presence service settings. This concerns in particular the following default presence statuses:

- Default presence status showing the availability by phone
- Private default presence status

These default presence statuses are shown to OpenScape users in the following situations:

- If an OpenScape user does not allow other users to see his/her actual presence status.
- If an OpenScape user has not yet replied to the request for letting his/her actual presence status see.

Start the configuration

Configure the presence service by executing in the CMP the following steps.

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click on the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Search the list for the **Presence Service** component and click on the associated component name.

The dialog with the presence service settings opens.

- 6) Specify one of the following values in the **Default Aggregated Media Presence Status** field.

Value	Default value for the aggregated media presence status
0	Unknown
1	Available
2	Busy
3	Offline

This setting defines the default value for the presence status showing the availability of OpenScape users by phone.

- 7) Specify one of the following values in the **Default User Preference for Subscriptions** field.

Value	Default value for the user presence status in case of viewing requests
0	Every request for viewing a user's presence status is automatically rejected. The OpenScape user who receives the request cannot allow showing his/her presence status.
1	Every request for viewing a user's presence status is automatically agreed to. The OpenScape user who receives the request cannot refuse showing his/her presence status.
2	The requested OpenScape user informed about the viewing request by a message. He/she can then decide for himself/herself whether or not to display his/her presence status.

This setting defines the OpenScape system default behavior in case a user is requested to show his/her presence status.

NOTICE: Every OpenScape user can customize this setting in his/her UC Application client.

- 8) Specify in the **Max Subscription** field how many presence statuses of other users each OpenScape user may monitor at most.

When this number has been reached for an individual OpenScape user, the OpenScape system automatically rejects all further viewing requests.

This setting allows limiting the system performance allocated for monitoring presence statuses.

- 9) If you do not use a Microsoft Lync connection, specify one of the following values in the **Default Presence Status** field.

Value	Default presence status
1	Do Not Disturb
2	Be Right Back
3	Unavailable
4	Busy
5	In meeting

Value	Default presence status
10	Available

This setting defines the default value for the private presence status of OpenScape users.

NOTICE: How to configure the presence service in case of an Lync connection will be described later in [Configuring the Presence Service](#).

- 10) Leave all other presence service settings unchanged and click on **Save** to copy the settings.

You have now configured the presence service.

4.6.9 Creating a User Profile

The profile management enables you to administer the access privileges for the OpenScape system in a standardized way. You find detailed information about the profile management concept in the *OpenScape Common Management Platform, Configuration and Administration* manual.

We recommend not to assign default profiles to users since these profiles allow only a very insufficient privilege gradation. Instead, you should create and use individual user profiles for operating the OpenScape system.

There are two methods of creating a new user profile.

- You can create an entirely new user profile
- You can copy an existing user profile and individually adapt its privileges.

Start the configuration

How to create an entirely new user profile:

- 1) Select in the **Domain** drop-down list of the CMP toolbar the domain in which you want to create the user profile.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **CMP** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **General > Profiles**.

A list of all user profiles configured in the selected domain appears in the workspace.

NOTICE: Please refer to [User Privileges for OpenScape UC Application](#) on page 719 , Configuration and Administration manual to see which functions are assigned to the UC Application default profiles **Essential**, **Professional** and **Team** and to the CMP administrator profiles.

- 4) Click **Add** to add a new profile.

The profile settings dialog opens.

- 5) Under **Name** enter a short, unique name for the new profile.

Under this name the profile is administered in the CMP.

- 6) Select under **Application** which privilege group the profile is to determine.

Which privilege groups are offered here for selection depends on the OpenScape components installed with the system. Possible privilege groups are:

- **CMP**

Contains the privileges for accessing the CMP

- **E/A-Cockpit**

Contains the E/A-Cockpit privileges

- **OpenScape Voice**

Contains the OpenScape Voice Assistant privileges

- **OpenScape UC App**

Contains the privileges for OpenScape UC Application

- **RGAssistant**

Contains the RG Gateways privileges

- **Symphonia**

Contains the privileges for the CMP

- **UM**

Contains the privileges for the OpenScape user management

- 7) Select the check boxes of the **privileges** you want to assign to the user profile.

The product names and licenses required for the activated rights are displayed in the **Licenses** area.

NOTICE: The OpenScape UC Application privileges are detailed in [User Privileges for OpenScape UC Application](#) on page 719.

- 8) Click on **Save** to copy the settings.

You have now created a new user profile.

NOTICE: The license database of the OpenScape system may at times contain contradictory information for a profile. As a result, the license control of the OpenScape system may withdraw privileges from users with this profile though such privileges are displayed in the profile management for the relevant profile. How to correct such database inconsistencies is described in [Synchronizing License Assignments anew](#) on page 580.

The general configuration steps are complete.

4.7 Configuring the Communications System Connection

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

You need to connect OpenScape UC Application to at least one communications system for using it. How to set up this connection depends on the communications system used.

The following sections describe the configuration steps that you need to execute for connecting the respective communications system or a mixed scenario.

- [Connecting OpenScape Voice](#)
- [Connecting an OpenScape 4000 System](#)
- [Connecting various Communications Systems simultaneously \(mixed Scenario\)](#)

After you have configured the communications systems used, you need to execute the following additional configuration steps:

- [Configuring Address Translation Contexts](#)
- [Address Translation – Configuring St. Routing](#)
- [Configuring the SIP Trunk in the OpenScape Media Server](#)
- [Creating User Accounts](#)

You find conceptual descriptions of how to connect communications systems to OpenScape UC Application in the *OpenScape UC Application, Planning Guide* manual.

4.7.1 Connecting OpenScape Voice

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice as communications system.

NOTICE: Only one OpenScape Voice system at the most can be connected to a UC Application system. In addition to the OpenScape Voice system, further OpenScape 4000 systems can be connected to the UC Application system.

NOTICE: Special requirements must have been complied with for connecting OpenScape Voice. See [Configuration requirements for OpenScape Voice](#) on page 81.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

How to connect OpenScape UC Application to OpenScape Voice:

- 1) [Checking OpenScape Voice Dependencies](#)
- 2) **For all deployment scenarios except for Integrated Deployment:**
[Configuring a reduced OpenScape Voice Assistant](#) if required
- 3) **For all deployment scenarios except for Integrated Deployment:**
[Configuring the OpenScape Voice System in the OpenScape Voice Assistant](#)
- 4) [Configuring the Synchronization of Business Group Data](#)
- 5) **For deployment scenarios with a single Media Server only:**
[Configuring the SIP Trunk in OpenScape Voice](#)

NOTICE: The corresponding configuration for provision scenarios with several OpenScape Media Servers occurs later in the sections: [Configuring the Conference Portal for Media Server Farm](#) on page 163 or [Configuring the Voice Portal for Media Server Farm](#) on page 189.

- 6) [Configuring the CSTA Link to OpenScape Voice](#)
- 7) [Configuring the Number of CSTA Sessions in OpenScape Voice](#)
- 8) [Configuring Office Codes](#)
- 9) [Configuring Prefixes](#)
- 10) **For deployment scenarios with independent Media Server computer systems only:**
[Configuring Packet Filters for Media Server Computer Systems](#)

These steps are described in detail in the following sections.

4.7.1.1 Checking OpenScape Voice Dependencies

Some OpenScape Voice features are excluded or restricted by the use of OpenScape UC Application. Before you start configuring OpenScape UC Application, you should therefore check the following conflict areas to rule out foreseeable problems.

NOTICE: A maximum of 50 services may be active in OpenScape Voice for each call. Five of these services are reserved for basic calls, so that in the end only 45 services are available per call.

- [General – OpenScape Voice](#)
- [Call Forwarding OpenScape Voice](#)
- [Caller ID OpenScape Voice](#)
- [User Mobility– OpenScape Voice](#)
- [Silent Monitoring Features OpenScape Voice](#)
- [Call Forwarding – Local Device](#)
- [Other general Elements OpenScape Voice](#)

The following table lists these conflict areas and points to foreseeable problems.

Possible support levels are:

- **Required**

The OpenScape UC Application functions require this OpenScape Voice feature to be active.

- **Supported**

The OpenScape UC Application functions work correctly, no matter whether or not this OpenScape Voice feature is active. If it is active, it can be operated using the UC Application clients.

- **Supported passively**

The OpenScape UC Application functions work correctly, no matter whether or not this OpenScape Voice feature is active. If it is active, it cannot be operated with the UC Application clients but with OpenScape Voice devices only.

- **Not recommended**

To ensure a uniform functionality, this OpenScape Voice feature should be disabled. The relevant function is enabled by OpenScape UC Application instead.

- **Not supported**

The OpenScape UC Application functions require this OpenScape Voice feature to be disabled.

General OpenScape Voice

Table 3: OpenScape Voice / UC Application Dependencies (General) (1)

Service	Recommendation
Hot Desking	Not supported.
Distinctive Ringing	Supported Restrictions apply only for the relevant device and not for other preferred devices of a UC Application user.
Night Bell Call Pickup Group	Supported passively.
Large Conference	Supported Registered OpenScape Voice SIP telephones are required for starting a device-controlled conference. There is no interaction between this feature and a UC Application conference, which is initiated and managed by UC Application clients and the conference portal of OpenScape UC Application.
Account Code	Supported passively.
Authorization Code	Not supported.

Service	Recommendation
CSTA	Required. Requires: Type 1 ⁵ for the endpoints optiPoint, optiClient 130 or OpenScape Desktop Client with SIP Provider CSTA Over SIP for OpenStage endpoints
Call Completion on No Reply	Supported passively.
Call Completion to Busy Subscriber	Supported passively.
Call Hold	Supported
Call Pickup Group	Supported passively.
Call Pickup Directed	Supported passively.
Call Transfer	Required.
Abandon Autom. Reversed-Charge Call	Supported
Automatic Collect Call Blocking	Supported

Table 4: OpenScape Voice / UC Application Dependencies (General) (2)

Service	Recommendation
Do Not Disturb	Not supported. Restrictions must be realized by OpenScape UC Application.
Executive Busy Override	Supported
Last Incoming Number Redial	Supported
Last Outgoing Number Redial	Supported
Line Restrictions	Supported Restrictions apply only for the relevant device and not for other preferred devices of a UC Application user.
Music On Hold	Supported
Anonymous Caller Rejection	Not recommended. Rules for handling calls should be realized by OpenScape UC Application.

⁵ In earlier OpenScape Voice versions this option is called **Siemens Type 1**.

Service	Recommendation
Selective Caller Acceptance	Not recommended. Rules for handling calls should be realized by OpenScape UC Application.
Selective Caller Rejection	Not recommended. Rules for handling calls should be realized by OpenScape UC Application.
Toll and Call Restrictions	Supported All UC Application users should be able to initiate international calls. All users should always use phone numbers in the international number format.
Speed Calling	Supported
BG Speed Dial	Supported
Multi-Contacts	Not recommended. Inconsistency of the user interface and feature restriction.

Call Forwarding OpenScape Voice

Table 5: OpenScape Voice / UC Application Dependencies (Call Forwarding)

Service	Recommendation
Call Forwarding - Busy	Supported
Call Forwarding - Dependable	Required when using non-registering devices otherwise recommended for backup routing in case application is not available.
Enhanced Call Forwarding	Not recommended. Is replaced with OpenScape UC Application.
Call Forwarding - No Reply	Supported
Remote Activation Call Forwarding	Not recommended. Is replaced with OpenScape UC Application.

Service	Recommendation
Selective Call Forwarding	Not recommended. Is replaced with OpenScape UC Application.
Call Forwarding - Unconditional	Supported
Call Forwarding to Voice Mail	Not recommended. Is replaced with OpenScape UC Application.
Call Forwarding Internal/External	Not recommended. Is replaced with OpenScape UC Application.
Call Forwarding, Remote Call Forwarding	Not supported.

Caller ID OpenScape Voice

Table 6: OpenScape Voice / UC Application Dependencies (Caller ID)

Service	Recommendation
Outgoing CID Suppression	Supported
Malicious Call Trace	Supported
Calling Name Permanent Presentation Status	Supported
Calling Number Permanent Presentation Status	Supported
Outgoing Call Presentation Status	Supported
Outgoing Call Presentation Status Plus	Supported
Calling Name Delivery Blocking	Supported
Calling Number Delivery Blocking	Supported

User Mobility OpenScape Voice

Table 7: OpenScape Voice / UC Application Dependencies (User Mobility)

Service	Recommendation
One Number Service	Required (coming and going).
Serial Ringing	Not supported.

Service	Recommendation
Simultaneous Ringing	Not supported.
Simultaneous Ringing Remote Activation	Not supported.

Silent Monitoring Features – OpenScape Voice

Table 8: OpenScape Voice / UC Application (SILM OpenScape Voice) dependencies

Service	Recommendation
Silent Monitoring Agent	Supported passively.
Silent Monitoring Protection	Supported passively.
Tagged for Monitor	Supported passively.
Silent Monitoring Supervisor	Supported passively.
Silent Monitoring Agent	Supported passively.

Call Forwarding – Local Device

Table 9: OpenScape Voice / UC Application Dependencies (Call Forwarding)

Service	Recommendation
Call Forwarding	Not recommended. Rules for handling calls should be realized by OpenScape UC Application.

Other general Elements OpenScape Voice

Table 10: OpenScape Voice / UC Application Dependencies (other general Elements)

Service	Recommendation
Hunt group as UC Application user	Not supported.

Service	Recommendation
UC Application user as hunt group target	Supported If a call arrives via hunt group and is transferred to the UC Application user, only the preferred device (OND) of the relevant UC Application user is called. If this transfer fails, the call is returned to the hunt group.
MLHG as preferred device, rules or routing target	Supported
National Numbering Plan	Not recommended.
International E.164 Numbering Plan	Supported
PNP Private Numbering Plan	Supported
Keyset	Not recommended. Only the primary line can be controlled by OpenScape UC Application; no secondary or phantom lines. OpenScape UC Application supports passive controlling of features for call-pickup groups. Passive support means that a user can configure a feature on his/her phone and OpenScape UC Application performs the setting and updates the UC Application accordingly. Such features cannot be configured in the UC Application GUI. Hunt groups are not supported with a keyset. You cannot reroute a call from a keyset line to a keyset-roll-over line by named device list. The Keyset feature is not supported by OSMO. If the Keysets feature is active on the OSV, when attempting to perform a network handover over Wi-Fi during an incoming ringing call, the OSV reports an <InvalidDestination> message in the 200 OK SIP response.

Service	Recommendation
Backup Routing	Supported

4.7.1.2 Configuring a reduced OpenScape Voice Assistant

NOTICE: The configuration steps of this chapter are optional. You can execute them if you do not use Integrated Deployment.

If in an OpenScape system the OpenScape components are distributed on several computer systems, it is not necessary to install a complete OpenScape Voice Assistant on each of the computer systems. It is sufficient to use a complete OpenScape Voice Assistant on only one of the computer systems. On all other computer systems, only parts of the OpenScape Voice Assistant are required.

NOTICE: If in case of redundant application computers, OpenScape Voice Assistant is intended to be used on the application computer, the complete OpenScape Voice Assistant must be installed on both application computers.

In this case, the OpenScape Voice system of the OpenScape system can only be configured and managed via the CMP the complete OpenScape Voice Assistant has been installed with.

If you want to use only a reduced OpenScape Voice Assistant on one of the OpenScape computer systems, configure it now. How to proceed is described in [Configuring a reduced OpenScape Voice Assistant](#) on page 565.

NOTICE: In the following descriptions, OpenScape Voice Assistant always refers to the complete OpenScape Voice Assistant of the OpenScape system.

4.7.1.3 Configuring the OpenScape Voice System in the OpenScape Voice Assistant

NOTICE: You must execute the configuration steps of this chapter only if you do not use Integrated Deployment.

NOTICE: The configuration steps of this chapter must be executed for every complete and every reduced OpenScape Voice Assistant.

You need to configure the connecting data of the OpenScape Voice system in the OpenScape Voice Assistant so that the OpenScape Voice Assistant can access the OpenScape Voice system.

Start the configuration

How to configure the connecting data of the OpenScape Voice system in the OpenScape Voice Assistant:

- 1) Start the CMP and log on with the **administrator@system** user ID.
- 2) On the **Configuration** navigation tab of the CMP click on the **OpenScape Voice** navigation menu item.
- 3) In the navigation tree, click on General > Switches.

A list of all OpenScape Voice systems configured in the OpenScape Voice Assistant is displayed.

- 4) Click **Add** to configure a new OpenScape Voice system in the OpenScape Voice Assistant.

The dialog with the link settings opens.

- 5) Under **Name** enter a short, unique name for the OpenScape Voice system.

Under this name the OpenScape Voice system will be managed in the CMP.

- 6) Specify the IP address *nafo0* in the **IP Address** field. This address has been configured for the OpenScape Voice system.

You find this setting in the following OpenScape Voice configuration file.

```
/etc/hic8000/node.cfg
```

- 7) In the **srx password** field specify the logon password for the srx user account of the OpenScape Voice system.

The default password of the srx user account of OpenScape Voice is **2GwN!gb4**.

- 8) Click on **Test Connection** to check whether the specified values allow access to the OpenScape Voice system.

The connection test should be successful.

- 9) Click on **Save** to copy the settings.

NOTICE: If this step fails though the connection test in the previous step was successful, you need to create a new firewall rule in OpenScape Voice before you can configure the connecting data of the OpenScape Voice system in the OpenScape Voice Assistant. How to proceed is described in [Creating a Firewall Rule in OpenScape Voice](#) on page 581.

You have now configured the connecting data of the OpenScape Voice system in the OpenScape Voice Assistant.

OpenScape UC Application already registers as CSTA application with OpenScape Voice.

4.7.1.4 Configuring Backup Routing feature for UC calls

Enable the Backup Routing attribute in order for OSV to initiate backup routing mechanism for OpenScape UC. Enable this option as with other uaCSTA connections, however CSTA over SIP applications do not use Application Session Services since they only manage a single device.

NOTICE: Starting with UC V11R3 FR9 Backup Routing is supported also with OpenScape 4000 V11R0. Prerequisite is to have To have Feature package 2021 active on OpenScape 4000 V11R0 (minimum RMX version V11R0.28.30 and CSTA V11R0.28.6) before backup routing is activated at UC side

Configuring the xml file:

In order to enable it, an instance file has to be modified as follows:

- 1) In a UC BE server (via ssh) search for the appropriate instance file inside folder /opt/siemens/common/conf/config-beans with the command:

```
grep AddressManagerImpl instance*
```
- 2) Once the file is found, open it for editing (e.g. with vi).
- 3) Find inside the property name
 "BACKUP_PREFERRED_DEVICE_ROUTING" and set its value to ON.

Configuring the CMP parameter:

Now you can proceed with the CMP configuration.

- 1) On the Configuration navigation tab of the CMP click on the OpenScape Voice navigation menu item.
- 2) Navigate to Signaling Management > CSTA. The CSTA Settings dialog opens.
- 3) Click on the Application tab and then click on the Interface Options tab.

The main purpose of the Interface Options tab is to provide a full backward compatibility for existing CSTA applications with the default attribute values.

You can see the list of all the Interface Attributes (with the indication if they appear for a V7 or a V8 OSV switch) that may be enabled or disabled for the selected application:

- 4) Enable Backup Preferred Device Routing.
 Value is disabled by default (unchecked).
- 5) Click Save.

IMPORTANT: When you enable this option, the CMP displays a warning, before enabling this option, stating: "Before modifying this CSTA Interface Option, verify that OpenScape UC Subscribers will not logon as OpenScape Contact Center Agents".

4.7.1.5 Configuring the Synchronization of Business Group Data

OpenScape UC Application adopts the data of all business groups configured in a connected OpenScape Voice system by default. However, taking the data of a single, selected business group is also possible.

NOTICE: Synchronizing single business groups is e. g. required if you wish to connect several UC Application systems to a shared OpenScape Voice system (multi-tenant environment).

Start the configuration

Execute the following steps for transferring the data of a single, selected business group to OpenScape UC Application:

- 1) Click on the **CMP** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on General > System Settings.
The dialog with the general system settings opens.
- 3) Select the **Use Domain to Business Group Mapping** option.

NOTICE: If you do not select this option, the data of all business groups is transferred to OpenScape UC Application.

- 4) Click on **Save** to copy the settings.
- 5) Click on the **OpenScape Voice** navigation menu item on the **Configuration** navigation tab of the CMP.
- 6) Select the **Business Group** entry.
- 7) In the navigation tree, click on Business Group List.
A list of all business groups configured in the OpenScape Voice is displayed.
- 8) Select the name of the business group the data of which shall be transferred to OpenScape UC Application.
The dialog with the settings of the selected business group opens.
- 9) In the **Domain** field, select the UC Application domain for which the business group data shall be transferred to OpenScape UC Application.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

NOTICE: Every UC Application domain can only be assigned to exactly one business group.

- 10) Click on **Save** to copy the settings.

Consequently, only the data of the selected business group is transferred to OpenScape UC Application.

4.7.1.6 Configuring the SIP Trunk in OpenScape Voice

NOTICE: You must execute the configuration steps of this chapter only if you use a single OpenScape Media Server entity in your deployment scenario. This may be the case either on the application computer or on a single Media Server computer. The corresponding configuration for provision scenarios with several OpenScape Media Servers occurs later in the sections: [Configuring the Conference Portal](#) on page 156 or [Configuring the Voice Portal](#) on page 182.

IMPORTANT: The OpenScape Media Server always requires an SIP trunk for communicating with OpenScape Voice. If no SIP trunk is configured in OpenScape Voice for the OpenScape Media Server, the communication between OpenScape Media Server and OpenScape Voice will fail.

OpenScape UC Application and OpenScape Voice communicate with each other via an SIP trunk to be configured between OpenScape Media Server and OpenScape Voice.

We recommend to use an individual numbering plan for configuring this SIP trunk in OpenScape Voice. You can then configure special numbering plan settings for this connection without influencing common OpenScape Voice subscribers.

This refers in particular to the **Display Number Modification** setting. This setting controls the format of the phone number transferred to the terminal device as originator number with a call. For common subscribers this is usually only the extension of a caller. For OpenScape UC Application must however the fully qualified E.164 phone number be transferred so that callers can be uniquely identified in OpenScape UC Application.

Start the configuration

How to configure the SIP trunk to the OpenScape Media Server in OpenScape Voice:

You find detailed information about how to configure OpenScape Voice in the OpenScape Voice Assistant documentation.

- 1) Select the numbering plan of the location the OpenScape Media Server is assigned to. If no appropriate numbering plan is available, create a new one.
- 2) Create a new end point profile for the business group in which you create the trunk to the OpenScape Media Server.
 - a) Select on the **General** tab under **Numbering Plan** the numbering plan you created in step 1.
 - b) Activate the following services under the service settings:
 - Voice Mail
 - Call Transfer
 - Call Forward Invalid Destinations
 - Toll and Call Restrictions
- 3) Create a new endpoint for the OpenScape Media Server.
 - Select type **Static** in the SIP settings.
 - In the SIP settings, specify as **Endpoint Address** the IP address under which the OpenScape Media Server can be reached.
 - Select the protocol OpenScape Voice is to use for the SIP communication with the OpenScape Media Server under Transport protocol on the **SIP** tab. The setting **Port** is automatically set to the default port of the selected transport protocol.

NOTICE: These values must correspond to the settings that you perform for the OpenScape Media Server SIP provider at

a later date (cf. [Configuring the SIP Trunk in the OpenScape Media Server](#) on page 144).

NOTICE: If the administrator performs any change to the Transport Protocol (TCP), it is strongly recommended that the WebRTC UC user is prompted to sign out and sign in again, in the application, to avoid implications.

- Activate the **Registered** option in the general settings.
 - Select the endpoint profile just created on the General tab.
 - Activate the **Allow Sending of Insecure Referred-By Headers** option in the attribute settings.
 - Activate the **Send International Numbers in Global Number Format (GNF)** option in the attribute settings. OpenScape Voice then sends all GNF-based phone numbers with a leading + character to the OpenScape Media Server.
 - Create under the alias settings a new alias for the IP address under which the OpenScape Media Server can be reached.
 - Create under the alias settings a new alias for the host name of the computer system on which the OpenScape Media Server is installed.
 - Configure the billing settings on the **Accounting** tab. This way, billing for ad-hoc conferences occurs via the ONS numbers.
 - Select in the billing settings under **Billing type** the **Miscellaneous** option.
- 4) Create a new destination for the route to the OpenScape Media Server and reopen the settings dialog for this destination.
- 5) Create a new route in the newly created destination.
- Select the **SIP Endpoint** entry for **Type**.
 - Select the **Undefined** entry for **Signaling type**.
 - In the **Number of digits to delete** field specify how many digits are to be cut off of an E.164 phone number before it is sent to the OpenScape Media Server.

NOTICE: This setting depends on how you configure the access numbers (address bindings) in the OpenScape Media Server at a later date. *Example:* Callers shall be able to reach the OpenScape Media Server voice portal under the E.164 phone number +49240490199100. In this case 99 is the network code in OpenScape Voice, via which calls are routed to the OpenScape Media Server. You configure the access number of the voice portal address binding as +492404901100. In this case the phone number portion 99 must be removed for the route to the Media Server. For the **Number of digits to delete** option you thus need to set number 2.

- Select the **International** entry for **Address type**.
- 6) Assign a prefix access code to the just created destination. For example, by adding a new E.164 code to the prefix access code that belongs to the office code.

- 7) Create a new rule for modifying the display number.
 - a) In the **Originating Context Settings** section, under **Business Group**, select option **ANY**.
 - b) In the **Terminating Context Settings** section, under **Endpoint**, select the endpoint you have just created for the OpenScape Media Server.
 - c) In the **Modification Rule** section, under **Input Type of Number**, select option **ANY**.
 - d) In the **Modification Rule** section, under **Output Type of Number**, select option **Normalized**.
 - e) In the **Modification Rule** section, under **Optimize Type of Number**, select option **None**.

You have now performed all settings in OpenScape Voice required for the SIP trunk between OpenScape Voice and OpenScape Media Server.

4.7.1.7 Configuring the CSTA Link to OpenScape Voice

OpenScape UC Application must monitor and control the OpenScape Voice devices. You need to configure a CSTA link between OpenScape Voice and each UC Application server for this purpose.

Start the configuration

How to configure a CSTA link between OpenScape UC Application and OpenScape Voice:

NOTICE: Most of the following settings have usually already been performed automatically by OpenScape Voice. Please check such automatically applied values.

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > OS Voice**.
A window opens, displaying all configured OpenScape Voice connections.
- 3) Click on **Add**.
The dialog with the link settings opens.
- 4) Select under **Switch** the OpenScape Voice system to be connected to OpenScape UC Application.
- 5) Select under **Version** the version of the OpenScape Voice system to be connected to OpenScape UC Application.
If you wish to use video conferences also, you need to select a version that ends in **Video**.
Example: OpenScape Voice Vx Video
- 6) Enter the IP address for the CSTA interface provided by OpenScape Voice in the **CSTA access configuration** area under **IP/Hostname**.
- 7) Specify port **1040** in the **CSTA access configuration** area in the **Port** field.

- 8) If OpenScape Voice provides an alternative CSTA interface, execute the following steps.
 - a) Enter the IP address for the alternative CSTA interface in the **IP/Hostname (alternative)** field of the **CSTA access configuration** area.
 - b) Specify port **1040** in the **Port (alternative)** field of the **CSTA access configuration** area.
- 9) Select a logical provider in the **BCom configuration** section under **Node** via which OpenScape Voice is to be connected.

Only one OpenScape Voice system can be connected to OpenScape UC Application via each logical provider.
- 10) Click on **Save** to copy the settings.

The new connection is saved and displayed in the connection list.

You have now configured the CSTA link between OpenScape UC Application and OpenScape Voice.

If required, you can check whether the CSTA connection between OpenScape UC Application and OpenScape Voice works correctly and OpenScape Voice devices are monitored. How to proceed is described in [Checking the CSTA Connection Function](#) on page 571.

NOTICE: During the system operation it may happen that CSTA connections are not properly closed. This causes the number of possible CSTA connections to be unavailable although these links are not used anywhere. Please refer to [Checking the Availability of CSTA Connections](#) on page 569 to learn how to track and solve this problem.

TLS Configuration for CSTA connectivity with OSV

BCOM CSTA Connector supports TLS1.2 (not MTLS) only on the OSV port 1041.

Follow the steps below to configure the CSTA port in UC via CMP:

- 1) Navigate to **Configuration > Unified Communications > Connections > OpenScape Voice > CSTA port**.
- 2) Set the CSTA port to 1041.

Next, you need to modify the CSTA level for OpenScape Voice via the CMP interface. For this, you must disable MTLS in the current port from OpenScape Voice.

- 1) Navigate to **Configuration > OpenScape Voice > Administration > Signaling Management > TLS Settings > CSTA**.
- 2) Change the CSTA level from **Trusted** to **None**.

4.7.1.8 Configuring the Number of CSTA Sessions in OpenScape Voice

OpenScape UC Application must monitor and control the OpenScape Voice devices. For this purpose, you configure a CSTA connection that uses two so-called CSTA sessions between OpenScape Voice and OpenScape-UC-Application.

OpenScape Voice restricts the number of possible CSTA sessions by a corresponding setting. Set an appropriate value for OpenScape Voice to allow a sufficient number of CSTA sessions.

NOTICE: If you use one OpenScape Voice system for several OpenScape environments, the number of CSTA sessions increases accordingly.

Provide for two additional sessions to compensate for sessions that may be blocked.

Start the configuration

How to configure the number of possible CSTA sessions in OpenScape Voice:

- 1) On the **Configuration** navigation tab of the CMP click on the **OpenScape Voice** navigation menu item.
- 2) In the navigation tree, click on **Administration > Signal Management > CSTA**.

The dialog with the settings of the CSTA management opens.

- 3) Specify the required number of CSTA sessions in the **Maximum CSTA Sessions** field.

If you use the OpenScape Voice system for a single OpenScape environment, enter **4**. Increase this number by two for each further OpenScape environment to use the same OpenScape Voice system.

NOTICE: The value range valid for the **Maximum CSTA Sessions** setting is from **1** to **256**.

- 4) Click on **Save** to copy the settings.

You have now configured the possible number of CSTA sessions in OpenScape Voice.

4.7.1.9 Configuring Office Codes

OpenScape UC Application retrieves all OpenScape Voice subscribers and their office codes. But UC doesn't retrieve the office codes with vacant DNs. So if there is no subscriber configured for an office code, the office code won't be retrieved by UC.

Furthermore you need to manually supplement the information copied in this way with additionally required data.

NOTICE: The change of Type of Number for OSV subscribers from public to private (or vice versa) doesn't change the type of UC devices from public to private (or vice versa). So if the Type of Number of an OSV subscriber is changed from public to private, the type of UC device will remain public on UC side. Instead of changing the Type of Number of an OSV subscriber from public to private, administrator should delete the OSV subscriber with the old Type of Number and recreate a new OSV subscriber with a new Type of Number.

Start the configuration

How to supplement the information of the OpenScape Voice office codes:

- 1) Select the desired domain from the **Domain** list in the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Devices > Office Codes**.
- 4) Use the **Comm.System** combo box to select the communications system for which you wish to supplement the office codes.

The workspace displays a list of all office codes that could automatically be copied from the database of the selected communications system.

NOTICE: If the list does not display all office codes configured in OpenScape Voice, this data has not been synchronized by OpenScape Voice yet. Synchronizing occurs once a day at night. To synchronize the office codes manually, reboot the OpenScape UC Application application computer. After the reboot you see a list of all OpenScape Voice office codes. The OpenScape Voice synchronization feature is detailed in the OpenScape Voice administration manual.

- 5) Click on the name of the first office code.

The dialog with the settings of the relevant office code opens.

- 6) Specify the overlap of the relevant office code in the **Overlap** field. This is in most cases **0**.

Example of determining the overlap:

A fully qualified phone number be 492404902100. The office code is 492404902 and the extension 2100. In this example, one digit of the extension and one of the office code overlap – namely digit **2**. The overlap for this example is thus 1.

- 7) Verify once again that the entry is correct.

NOTICE: You can save the **Overlap** value again only once.

- 8) Click on **Save** to copy the settings.
- 9) Execute steps 5 to 8 also for all other office codes displayed in the workspace.

You have now supplemented the office codes with all required additional information.

4.7.1.10 Configuring Prefixes

OpenScape UC Application copies the OpenScape Voice prefixes automatically from the OpenScape Voice database. But you need to manually supplement the information copied in this way with additionally required data.

Start the configuration

How to supplement the information of the OpenScape Voice prefixes:

- 1) Select the desired domain from the **Domain** list in the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Devices > Prefixes**.
- 4) Use the **Comm.System** combo box to select the communications system for which you wish to supplement the prefixes.

The workspace displays a list of all prefixes that could automatically be copied from the database of the selected communications system.

NOTICE: If the list does not display all prefixes configured in OpenScape Voice, this data may not have been synchronized by OpenScape Voice yet. You define the time at which OpenScape Voice synchronizes its database in the OpenScape Voice Assistant switch-individually with the setting **Synchronization will start** at the following point:
General > <Edit switch >

The administrator manual for OpenScape Voice describes details of the OpenScape Voice synchronization feature.

- 5) Click on the name of the first prefix.

The dialog with the settings of the relevant prefix opens.

- 6) Enter the missing settings for the prefix.

NOTICE: You find information about prefix settings in the documentation for the relevant communications system.

- 7) Click on **Save** to copy the settings.
- 8) Execute steps 5 to 8 also for all other prefixes displayed in the workspace.

You have now supplemented the prefixes plans with all required additional information.

4.7.1.11 Configuring Packet Filters for Media Server Computer Systems

NOTICE: You need to execute the configuration steps of this chapter only if you use at least one independent Media Server computer system.

Each OpenScape Media Server communicates with OpenScape Voice via the SOAP ports 8767 and 8768. These ports are blocked by the firewall of OpenScape Voice. To open them you need to configure new packet filter rules in OpenScape Voice. In this process you can assign any names to the packet filter rules.

Start the configuration

How to create the new packet filter rules in OpenScape Voice:

- 1) Start as user **srx** startCli of OpenScape Voice.
- 2) Log on as **sysad**.
- 3) Select 6 (Application Level Management).
- 4) Select 8 (Network Element Security Management).
- 5) Select 4 (Packet Filter Rules Security Management).
- 6) Select 1 (Create).
- 7) Enter the following settings for the new packet filter rule:
 - Remote IP Address:
<IP address of the OpenScape Media Server>
 - Transport Protocol:
3 (TCP)
 - Remote Port Begin:
0 (All Ports)
 - Direction:
1 (incoming)
 - Local Host:
bond_node_alias
 - Local Port Begin:
8767
 - Local Port End:
0 (Only Local Port Begin Valid)
 - Action:
1 (Allow)
- 8) Adopt the new packet filter rule.
- 9) Select 1 (Create).

10) Enter the following settings for the new packet filter rule:

- Remote IP Address:
<IP address of the OpenScape Media Server>
- Transport Protocol:
3 (TCP)
- Remote Port Begin:
0 (All Ports)
- Direction:
1 (incoming)
- Local Host:
bond_partner_alias
- Local Port Begin:
8767
- Local Port End:
0 (Only Local Port Begin Valid)
- Action:
1 (Allow)

11) Adopt the new packet filter rule.**12)** Select 1 (Create).**13)** Enter the following settings for the new packet filter rule:

- Remote IP Address:
<IP address of the OpenScape Media Server>
- Transport Protocol:
3 (TCP)
- Remote Port Begin:
0 (All Ports)
- Direction:
1 (incoming)
- Local Host:
bond_node_alias
- Local Port Begin:
8768
- Local Port End:
0 (Only Local Port Begin Valid)
- Action:
1 (Allow)

14) Adopt the new packet filter rule.**15)** Select 1 (Create).

16) Enter the following settings for the new packet filter rule:

- Remote IP Address:
<IP address of the OpenScape Media Server>
- Transport Protocol:
3 (TCP)
- Remote Port Begin:
0 (All Ports)
- Direction:
1 (incoming)
- Local Host:
bond_partner_alias
- Local Port Begin:
8768
- Local Port End:
0 (Only Local Port Begin Valid)
- Action:
1 (Allow)

17) Adopt the new packet filter rule.

18) Create the described packet filter rules for each computer system on which an OpenScape Media Server is installed.

19) Select 4 (display) to check the settings of the configured packet filter rule once more.

The required SOAP ports are thus open in OpenScape Voice for the OpenScape Media Server.

You have now connected OpenScape Voice to OpenScape UC Application.

4.7.1.12 Enabling Call Forwarding for Internal and External Originators for OpenScape Voice Subscribers

To allow an OpenScape Voice subscriber to configure their system to forward calls based on their origin (internal or external), it is mandatory to perform the following configuration in subscriber's Features profile.

- 1) Open CMP and navigate to **Configuration > OpenScape Voice**.
- 2) Scroll through the list of subscribers and locate the desired one or search for it using the search field.
- 3) Click the subscriber you want to configure.

A new window opens and you can edit subscriber's configuration.

- 4) Select the **Features** tab, then locate the **Subscriber Features** area. Click the box next to **Feature Name** and select **Call Forwarding Internal/External** from the drop-down menu.

A new window opens and you can edit the call forwarding configuration for internal and external originators.

- 5) Select the **General** tab, locate the **Activate** area, then check the box next to the **Activate** option.

- 6) Locate the **Forward All Calls** area and enable the following options:
 - **Allow Endpoint Control Internal**
 - **Allow Endpoint Control External**
- 7) Select the **Advanced** tab.
- 8) Locate the **Forward on Busy** area and enable the following options:
 - **Allow Endpoint Control Internal**
 - **Allow Endpoint Control External**
- 9) Locate the **Forward on No Answer** area and enable the following options:
 - **Allow Endpoint Control Internal**
 - **Allow Endpoint Control External**

4.7.2 Connecting an OpenScape 4000 System

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape 4000 as communications system

NOTICE: Not more than 120 OpenScape 4000 systems can be connected to a UC Application system. In addition to the OpenScape 4000 systems, one more OpenScape Voice system at the most can be connected to the UC Application system.

NOTICE: Special requirements must have been complied with for connecting OpenScape 4000. See [Configuration requirements for OpenScape 4000](#) on page 81.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

How to connect OpenScape 4000 to OpenScape UC Application:

- 1) [Configuring the SIP Trunk in OpenScape 4000](#)
- 2) [Activating the Import / Export-API in OpenScape 4000 Assistant](#)
- 3) **If you wish to connect several OpenScape 4000 systems to OpenScape UC Application using a OpenScape 4000 manager:**

[Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager](#)

- 4) [Configuring a CSTA Connection to an individual OpenScape 4000 System](#)

These steps are described in detail in the following sections.

4.7.2.1 Configuring the SIP Trunk in OpenScape 4000

IMPORTANT: The OpenScape Media Server always requires an SIP trunk for communicating with OpenScape 4000. If no SIP trunk is configured in OpenScape 4000 for the OpenScape Media Server, the communication between OpenScape Media Server and OpenScape 4000 will fail.

OpenScape UC Application and OpenScape 4000 communicate with each other via an SIP trunk to be configured between OpenScape Media Server and the HG 3500 module of the OpenScape 4000 system.

To configure this SIP trunk in OpenScape 4000 you need to create a native SIP trunk there. In doing so please heed the following:

- If you wish to connect OpenScape Xpressions to OpenScape UC Application, you need to use the phone number format **Unknown / Unknown** for the native SIP trunk.
- If you do not wish to connect OpenScape Xpressions to OpenScape UC Application, you should use the phone number format **ISDN / International** for the native SIP trunk.

The product information for OpenScape 4000 describes how to configure the native SIP trunk in OpenScape 4000.

You find conceptual descriptions of how to connect several OpenScape 4000 systems to OpenScape UC Application in the *OpenScape UC Application, Planning Guide* manual.

4.7.2.2 Activating the Import / Export-API in OpenScape 4000 Assistant

The OpenScape 4000 connection uses the import / export API (XIE API) of OpenScape 4000 Assistant for transferring data from OpenScape 4000 to OpenScape UC Application. This import / export API must be active in OpenScape 4000 Assistant,

which should be the case by default.

Start the configuration

How to check whether the import / export API in OpenScape 4000 Assistant is active:

- 1) Start OpenScape 4000 Assistant.
- 2) Select **Base Administration > Application Control** in the launch pad.
- 3) The check box of the **Import / Export API (XIE)** application should be active.

4.7.2.3 Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager

NOTICE: You need to execute the configuration steps of this chapter only if you wish to connect several OpenScape 4000

systems administered via a central OpenScape 4000 manager to OpenScape UC Application.

If you use several OpenScape 4000 systems and administer them via a central OpenScape 4000 manager, prepare connecting these OpenScape 4000 systems by configuring a connection between OpenScape 4000 manager and OpenScape UC Application.

In this way, the configuration elements for the single OpenScape 4000 systems are automatically created in the OpenScape UC Application database. Hence you save creating the single OpenScape 4000 connections individually.

IMPORTANT: You need to ensure that the communication between the application computer of OpenScape UC Application and the OpenScape 4000 manager is not restricted by a firewall.

Start the configuration

How to configure a connection to the OpenScape 4000 manager on the OpenScape UC Application side:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes**.

You see all nodes that are available in the OpenScape system.

- 3) Click on **Add HiPath 4000**.

The dialog with the node settings opens.

- 4) Select under **This node is:** the **Manager** option that matches your OpenScape 4000 version used.
- 5) Specify under **Name** a short, unique name for the connection to the OpenScape 4000 manager.

Under this name the connection to the OpenScape 4000 manager is administered in the CMP.

- 6) Specify under **IP address/Hostname** the IP address under which the OpenScape 4000 manager can be reached.
- 7) **For OpenScape 4000 V7:** Check that port number **443** is specified under **Administration Port**.
- 8) Specify under **User Name** the name of the user account that can be deployed for accessing the OpenScape 4000 manager.
- 9) Specify under **Password** the password for the specified user account.
- 10) Click on **Save** to copy the settings.

The new connection to the OpenScape 4000 manager is saved and displayed in the node list. At the same time, the names of all OpenScape 4000 systems are transmitted to OpenScape UC Application via port 4444 of the OpenScape 4000 manager's element manager.

A new configuration element is created in the OpenScape UC Application database for each OpenScape 4000 system. This element is displayed in the node list as additional node. However, the settings of these configuration elements must still be adjusted to the individual system environment. How to proceed is described in the following [Configuring a CSTA Connection to an individual OpenScape 4000 System](#) on page 136.

4.7.2.4 Configuring a CSTA Connection to an individual OpenScape 4000 System

OpenScape UC Application must monitor and control the OpenScape 4000 devices. You need to configure a CSTA link between OpenScape 4000 and OpenScape UC Application for this purpose.

IMPORTANT: You need to ensure that the communication between the application computer of OpenScape UC Application and the OpenScape 4000 system is not restricted by a firewall.

If you wish to connect several OpenScape 4000 systems with a OpenScape 4000 manager to OpenScape UC Application directly, you need to have executed the steps from [Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager](#) on page 134. After you have performed the configuration described there, the configuration elements required for the various OpenScape 4000 systems are automatically created in the OpenScape UC Application database.

Hence you save creating the single OpenScape 4000 connections individually. You only need to adjust the settings of the relevant configuration elements to the individual system environment.

Start the configuration

How to configure a CSTA connection to the OpenScape 4000 system on the OpenScape UC Application side:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes**.
You see all nodes that are available in the OpenScape system.
- 3) Execute one of the following steps depending on whether or not you have already connected a OpenScape 4000 manager in the previous section.
 - **If you have not connected an OpenScape 4000 manager:**
Click on **Add HiPath 4000** to create a new node for connecting a OpenScape 4000 system manually.
 - **If you have already connected an OpenScape 4000 manager:**
Click on the name of a node entry already automatically created for a OpenScape 4000 system.
- 4) Check that under **This node is:** the **self managed** option that matches your OpenScape 4000 version used has been selected.
- 5) Specify under **Name** a short, unique name for the node.
Under this name the node is administered in the CMP.
- 6) Specify under **IP address/Hostname** the IP address under which the HiPath Assistant can be reached.
- 7) **For OpenScape 4000 V7:**
Check that port number **443** is specified under **Administration Port**.
- 8) Specify under **User Name** the name of the user account that can be deployed for accessing the OpenScape 4000 system.
- 9) Specify under **Password** the password for the specified user account.
- 10) Specify under **SNMP Read Community** the name of the community created in the OpenScape 4000 system.

- 11) Specify under **CSTA IP** the IP address under which the CSTA interface of the OpenScape 4000 system can be reached.
- 12) Specify under **CSTA Port** the port number of the OpenScape 4000 application to be used for connecting OpenScape UC Application.
- 13) Click on **Save** to copy the settings.

The settings for the OpenScape 4000 node are saved and displayed in the node list.

You have now configured the CSTA connection to OpenScape 4000. At the same time, all required resource information of the relevant OpenScape 4000 system was transferred to the OpenScape UC Application database.

- 14) If you wish to connect several OpenScape 4000 systems to OpenScape UC Application manually, or if nodes were automatically created for several OpenScape 4000 systems in the previous section, configure the nodes of all OpenScape 4000 systems to be connected in the described manner.

You have now connected OpenScape 4000 to OpenScape UC Application.

4.7.2.5 Enabling Call Forwarding for Internal and External Originators for OpenScape 4000 Subscribers

For OpenScape 4000 subscribers, it is only possible to configure call forwarding for internal and external originators for the **Always forward** mechanism. By default, the **Call Forward Busy** and **Call Forward No Reply** configurations do not support internal and external call originators.

To allow an OpenScape 4000 subscriber to configure **Always forward** for internal and external originators, the following configuration steps must be performed:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

You can find this file in the following folder of the application computer:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

- 2) Set the value of the **callForwarding.allowCFWIntExtOnlyForAlwaysFwd** property to **true** to enable this feature.

`callForwarding.allowCFWIntExtOnlyForAlwaysFwd = true`

The default value is **false**.

- 3) Save the changes in the configuration file.

4.7.3 Connecting various Communications Systems simultaneously (mixed Scenario)

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice and OpenScape 4000 as communications system simultaneously.

NOTICE: Special requirements must have been complied with for connecting OpenScape Voice. See [Configuration requirements for OpenScape Voice](#) on page 81.

NOTICE: Special requirements must have been complied with for connecting OpenScape 4000. See [Configuration requirements for OpenScape 4000](#) on page 81.

How to connect OpenScape Voice and OpenScape 4000 to OpenScape UC Application simultaneously:

- 1) [Configuring the Trunk between OpenScape Voice and OpenScape 4000](#)
- 2) [Configuring the OpenScape Voice Connection](#)
- 3) [Configuring the Connection to OpenScape 4000](#)

4.7.3.1 Configuring the Trunk between OpenScape Voice and OpenScape 4000

The mixed scenario assumes that OpenScape Voice is connected to the OpenScape 4000 systems used via a trunk. Configuring such trunks is independent from OpenScape UC Application and therefore presupposed for the following configuration steps.

How to connect OpenScape Voice to OpenScape 4000 via a trunk describes the *OpenScape UC Suite, Solution Test Configuration Manual*, for example.

4.7.3.2 Configuring the OpenScape Voice Connection

To configure OpenScape Voice for the mixed scenario you first need to ensure the following in OpenScape Voice:

- Implicit phone numbers (<access code> + <prefix> + <phone number>) must be dialable.
- Explicit phone numbers must be used for external calls, because external communications systems do not have any information about prefixes and access codes to be used.

That means:

- For calls that reach OpenScape Voice from outside:
 - The originator numbers must be correctly normalized by OpenScape Voice. You find the required settings in the CMP under **Display Number Modification > Normalizations**.

You find continuative information about these settings in the *OpenScape Voice, Administrator Documentation* manual.

- For calls that OpenScape Voice transfers to the external:
 - For each explicit, external called directory number, the prefix access code, destination code and destination must be configured in OpenScape Voice.
 - OpenScape Voice must remove prefixes and access codes from an explicit, external called directory number before it transfers the called directory number to an external communications system.
 - The originator numbers must be correctly normalized by OpenScape Voice. In the CMP, under **Display Number Modification > Definitions**, you must configure entries the office codes of which correspond to the directory numbers configured in OpenScape Voice for this purpose.

You find continuative information about these settings in the *OpenScape Voice, Administrator Documentation* manual.

- For calls to the OpenScape Media Server:
 - In the CMP, under **Display Number Modification > Modifications**, you must add a general rule to OpenScape Voice that effects the phone numbers of incoming calls being transferred to the OpenScape Media Server in normalized format. Select the **Normalized** option for the rule setting **Output Type Of Number** for this purpose.

You find continuative information about these settings in the *OpenScape Voice, Administrator Documentation* manual.

In a mixed scenario, OpenScape Voice is connected exactly in the same way as connecting OpenScape Voice to OpenScape UC Application exclusively.

Therefore, execute the configurations steps from the following chapter to connect OpenScape Voice to OpenScape UC Application.

[Connecting OpenScape Voice](#) on page 111

4.7.3.3 Configuring the Connection to OpenScape 4000

To configure OpenScape 4000 for the mixed scenario you first need to ensure the following in OpenScape 4000:

- Implicit phone numbers (<access code> + <prefix> + <phone number>) must be dialable. This requires configuring LDPLN, LDAT and ODR.
- The explicit format must be used for external called directory numbers. Consequently, OpenScape 4000 must remove prefixes and access codes from called directory numbers before it transfers a called directory number to OpenScape Voice.

- In OpenScape 4000, number modification is configured. This requires you to configure the following:
 - Using AMO KNPRES, the exit codes and prefixes of the node, so that the calling and called directory numbers are used with their exit codes and prefixes.
 - Using AMO KNDEF, the various codes (country code, area code etc.), so that calling and called directory numbers are used in normalized format.

You find continuative information about these settings in the manual *OpenScape 4000 Volume 1 – AMO Descriptions, Service Documentation*.

In a mixed scenario, OpenScape 4000 is connected to OpenScape UC Application via an ACL or CSTA connection only.

To this, execute the following configuration steps from [Connecting an OpenScape 4000 System](#) on page 133.

- 1) [Activating the Import / Export-API in OpenScape 4000 Assistant](#)
- 2) **If you wish to connect several OpenScape 4000 systems to OpenScape UC Application using a OpenScape 4000 manager:**

[Adding CSTA Connections to several OpenScape 4000 Systems using an OpenScape 4000 Manager](#)

- 3) [Configuring a CSTA Connection to an individual OpenScape 4000 System](#)

4.7.4 Configuring Address Translation Contexts

UC Application components process phone numbers internally always in the so-called normalized phone format – example: +492404901100. A phone number in this format is either globally unique and based on the Global Number Format (GNF, E.164-based), or it has a private normalized format.

Processing a phone number exclusively in the normalized format has the following advantages:

- The phone number contains all information that uniquely identifies it. This enables optimum phone number evaluation.
- All UC Application components can work with a fixed phone number format, which simplifies exchanging phone numbers within the system.

If an UC Application component receives a non-normalized phone number, the relevant component uses an algorithm to normalize this phone number before its further processing. If, on the other hand, a normalized phone number shall be transferred to an external system or played to a user, a comparable algorithm is used to convert this phone number in a format that the relevant external system or a user deploys. This process is called localization.

A phone number is always normalized or localized in the scope of one of the following contexts:

- In a user-related context
- In a server-related context

- User-related contexts Phone number normalization or localization in the user-related context is required, for example, in the following cases:
 - When a user transfers a phone number to the OpenScape system and this phone number needs to be normalized for further processing.
 - When the OpenScape system puts out a normalized phone number to a user in a user-friendly format.

A user-related context is described either via the settings of a user account or by a global phone number.

Beyond that, no further configuration is necessary.

- Server-related contexts Phone number normalization or localization in the server-related context is required, for example, in the following cases:
 - When an external system transfers a phone number to the OpenScape system and this phone number needs to be normalized for further processing.
 - When the OpenScape system transfers a normalized phone number to an external system but this system does not expect a normalized but an individual phone number format.

A server-related context is described by a so-called address translation context. Any number of such address translation contexts can be configured. They are configured by the administrator in the CMP.

Phone number normalizations or localizations based on address translation contexts are performed, for example, by UC Application components that connect external systems to OpenScape UC Application – for example by the groupware connector or the OpenScape Media Server.

Start the configuration

How to configure an address translation context valid across the system:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Address Translation Contexts**.

You see a list of all address translation contexts configured in the OpenScape system.

- 3) Select **Add**.

The configuration dialog for creating an address translation context opens.

- 4) Verify that the **Context** tab is displayed.
- 5) Under **Name**, enter a short, unique name for the new address translation context.

Under this name the address translation context is administered in the CMP.

- 6) Specify a short **Description** for the address translation context.
- 7) Under **Switch**, select the communications system the numbering or dialing plans of which shall serve as base for the address translation context.

This field offers all communications systems connected to OpenScape UC Application for selection.

- 8) Select under **Public Office Code** the office code the address translation context is to use for normalizing public phone numbers.

- 9) Select under **Private Office Code** the office code the address translation context is to use for normalizing private phone numbers.
- 10) Select the unknown office code under **Unknown Office Code** as far as available.

It is used for example in case of an open or virtual numbering (VNR).

NOTICE: On the **UI & IT Norm.** tab you can select groovy scripts that control phone number normalization or localization. Because the supplied versions of selectable Groovy scripts are merely empty script containers, OpenScape UC Application replaces them with system-integrated scripts that cannot be customized. In order to avoid using the system-integrated scripts of OpenScape UC Application, the script containers supplied by default can be filled with customized Groovy scripts. Please consult Professional Services & Solutions (PS & S) of Unify Software and Solutions GmbH & Co. KG for such script adjustments.

- 11) Click on **Save** to copy the settings.
- 12) If the directly connected communications systems use several office codes, create an individual address translation context for each office code in the described manner.
- 13) Check that the **Set as default context** option is active for one of the configured address translation contexts.

You have now created the required address translation contexts. Such contexts will later be referenced in the station routing of the address translation or in the SIP trunk of the OpenScape Media Server.

4.7.5 Address Translation – Configuring St. Routing

If you connect at least one OpenScape 4000 system to OpenScape UC Application directly, you must configure the address translation by means of station routing.

OpenScape UC Application uses the address translation by means of station routing for the following purposes:

- To create a complete phone number from a simple extension (phone number normalization)
- To determine the extension from a complete phone number (phone number localization) if required

To achieve this, the address translation assigns an office code to each extension by means of station routing.

Before you can configure address translation by station routing, you must have created address translation contexts as described in [Configuring Address Translation Contexts](#) on page 140.

Which station routings do you have to configure?

NOTICE: In the following, the local system will describe the system in which calls or other actions take their origin.

Please note the following hints to determine the station routings you must configure:

- If you do not use a OpenScape 4000 system with the UC Application system, you do not have to configure any station routings.
- If you use only a single OpenScape 4000 system with the UC Application system and only extensions may be dialed, you must configure station routings for all extensions of the local system.
- If you use several OpenScape 4000 systems with closed numbering plan with the UC Application system and extensions may be dialed via network routing, you must configure station routings for all extensions of the local system and for all extensions of the target systems.
- If you use several OpenScape 4000 systems with closed numbering plan with the UC Application system and public dialing via network routing, you must configure station routings for all extensions of the local system.
- If you use several OpenScape 4000 systems with open numbering plan with the UC Application system and extensions may be dialed via network routing (*node access code + extension*), you must configure station routings for all extensions of the local system and for all extensions of the target systems. In this process, you must specify the address ranges in the format *NAC + extension*.
- If you use several OpenScape 4000 systems with open numbering plan with the UC Application system and public dialing via network routing, you must configure station routings for all extensions of the local system.
- If you use at least one OpenScape 4000 system with virtual numbering plan (VNR) with the UC Application system, you must configure the station routings for all extensions of all virtual nodes of the local system. In this process, you must specify the address ranges in the format *NAC + extension*.
- If you use OpenScape Voice and any number of OpenScape 4000 systems with the UC Application system, you must configure station routings for the OpenScape Voice target system.

Start the configuration

How to define station routings:

- 1) Select the desired domain from the **Domain** list in the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Configuration > Address Translation St. Routing**.
- 4) Click on **Add** to configure a new station routing.
The window for adding a station routing opens.
- 5) Select the communications system in the context of which extensions shall be considered from the **Communication System** field.
- 6) Select the **Extension** option in the **Type** field.
- 7) Select the address translation context that contains the target system's office code in the **Context** field.

- 8) Using **Range Start** and **Range Stop** define the extension range.

If the extension range is not cohesive, create several station routings.

- 9) Click on **Save** to copy the settings.

You have now defined the required station routings.

4.7.6 Configuring the SIP Trunk in the OpenScape Media Server

IMPORTANT: The OpenScape Media Server always requires an SIP trunk for communicating with a communications system. If no SIP trunk is configured in the communications system for the OpenScape Media Server, the communication between OpenScape Media Server and the communications system fails.

OpenScape UC Application and a communications system communicate with each other via an SIP trunk that needs to be configured between OpenScape Media Server and the communications system.

In this section you configure the SIP trunk on the OpenScape Media Server side. You need to configure the SIP provider of the OpenScape Media Server for this purpose.

If the OpenScape Media Server shall set up outbound SIP connections even if a communications system connected in such a way fails, you can optionally connect further alternative communications systems to the OpenScape Media Server also.

If you use several OpenScape Media Servers in your deployment scenario, you need to execute the configuration steps of this chapter on each OpenScape Media Server used.

If you wish to connect several communications systems to OpenScape UC Application directly, you need to execute the configuration steps of this chapter for each of the communications systems to be connected directly.

Start the configuration

Configure in the OpenScape Media Server the SIP trunk to the communications system by executing the following steps.

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) Click on the name of the OpenScape Media Server that you want to connect to the communications system.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

- 5) In the provider list select the link **IP Telephony (SIP)**.

The configuration dialog with the SIP provider settings opens.

SIP trunks on the OpenScape Media Server side are configured in this dialog in the form of SIP servers.

- 6) To do this, select **Add** in the **SIP Servers** section.

A configuration dialog in which you can configure a new SIP server for outbound communication connections opens.

- 7) Specify a short, unique name for the new SIP server in the **ID** field.

The SIP server will be administered under this name in the SIP provider settings.

- 8) In the **SIP Server Name (FQDN / IP Address)** field specify the IP address of the communications system that the OpenScape Media Server is to use for outgoing connection requests.

- For OpenScape Voice this is the IP address of the SIP service manager (SIP SM) of node 1.

NOTICE: You can determine this IP address in the CMP in the following location: **Configuration > OpenScape Voice > Administration > Signaling Management > SIP** in the **Node 1 Listening IP Address 1 for UDP, TCP and TLS** field. OpenScape Voice endpoints do not use TLS by default. To use TLS, you need to set the MTLS transport protocol for the relevant endpoints via the OpenScape Voice Assistant or via the startCli console of OpenScape Voice.

- For OpenScape 4000 this is the IP address of the HG module used.

If the host name of the associated computer system can be resolved into the relevant IP address in the network, you can also enter the associated host name instead of the IP address.

- 9) Enter the **Port number** configured on the relevant communications system for the SIP communication in the corresponding field.

If it uses the transport protocol UDP or TCP for the SIP communication, enter port **5060**. If it uses TLS as transport protocol, enter port **5061**.

NOTICE: If the same IP address is configured for SIP TLS and SIP MTLS in OpenScape Voice, the MTLS listening point uses the port number 5161. You can determine the configuration of the relevant IP addresses in the CMP in the following location: **Configuration > OpenScape Voice > Administration > Signaling Management > SIP**.

- 10) In the **Address translation context** field select the name of the address translation context that the OpenScape Media Server is to use for SIP communication with the communications system in case of outgoing calls.
- 11) In the **Listening Point ID** field select the ID of the listening point that the OpenScape Media Server is to use for the SIP communication with the communications system in case of outgoing calls.

NOTICE: OpenScape Voice endpoints do not use TLS by default. To use TLS, you need to set the **MTLS** transport protocol for the relevant end points via the OpenScape Voice Assistant or via the CLI console of OpenScape Voice.

12) How to configure alternative SIP servers for the SIP server just configured:

In doing so please note:

- In case of a co-located OpenScape Voice system you must not configure any alternative SIP servers.
- In case of a geo-separated OpenScape Voice system you may configure exactly one alternative SIP server. This should be the SIP Service Manager (SIP SM) of the associated node 2.

NOTICE: You can determine whether to use OpenScape Voice as co-located or geo-separated system in the CMP in the following location: **Configuration > OpenScape Voice > General > Switches** If the **Switch Type** column displays type **Duplex**, the system is a co-located one. Type **Geographically Separated Duplex** is displayed for a geo-separated system.

a) Select **Add** under **Alternative SIP servers**.

A configuration dialog in which you can configure an alternative SIP server for the just configured one opens.

b) In the **SIP Server Name (FQDN / IP Address)** field specify the IP address of the alternative communications system that the OpenScape Media Server is to use for outgoing connection requests if required.

In case of a geo-separated OpenScape Voice system this is the IP address of the SIP Service Manager (SIP SM) of the associated node 2.

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

c) Enter the **Port number** configured on the alternative communications system for the SIP communication in the corresponding field.

As a rule, this is the same port number you used in step 9.

d) Select **Save** to copy the modifications.

e) If required, configure further alternative SIP servers.

13) Select **Save** to copy the modifications.

You have now modified the SIP provider settings used for outgoing connections.

For incoming connections the SIP provider uses the following listening points by default:

Binding address	Port number	Transport protocol
<is automatically determined>	5060	UDP
<is automatically determined>	5060	TCP

<is automatically determined >	5061	TLS

With these settings for inbound connections the SIP provider is already operable. You need not configure the settings.

NOTICE: These values must correspond to the settings you have configured in the communications system for the SIP trunk.

- 14) Select Close.
- 15) Select the radio button of the **IP Telephony (SIP)** provider and select **Restart Provider**.
- 16) If you use several OpenScape Media Servers in your deployment scenario, execute steps 1 to 15 on each of the OpenScape Media Servers used.
- 17) If you wish to connect several communications systems to OpenScape UC Application directly, execute steps 1 to 16 for each of the communications systems to be connected directly.

You have now performed all settings in the OpenScape Media Server required for the SIP trunk between the OpenScape Media Server and the communications system .

The communications systems used are now connected to OpenScape UC Application.

4.7.7 Creating User Accounts

You need to create a user account in the CMP for each OpenScape user. This applies for every OpenScape user, no matter which communications system he/she deploys.

There are two methods of creating a new user account.

- The user management of the CMP lets you provide user accounts from the communications systems OpenScape Voice and OpenScape 4000. How to proceed is described in the *OpenScape Common Management Platform, Administrator Documentation*.
- The user management of the CMP allows providing user accounts with the help of the import function. How to proceed is described in the *OpenScape Common Management Platform, Administrator Documentation*.
- You can create user accounts manually.

NOTICE: When you create a new user account, approximately 10 minutes must pass before a user can log on to the OpenScape Web Client via this user account.

Start the configuration

How to create a new user account manually:

- 1) Select in the **Domain** drop-down list of the CMP toolbar the domain in which you want to create the user account.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Accounts > List**.

A list of all users configured in the selected domain appears in the workspace.

- 4) Click on **Add**.

The user settings dialog opens.

- 5) Enter the following data on the **General** tab.

- **Login name**

User ID of the user. This name is used for logging on to the system.

Do not use any of the following characters in the login name:

- @
- Semicolon
- Blank
- Tabulator
- Capital letter
- Apostrophe

NOTICE: The system automatically converts capital letters in small letters.

- **Name**

Name of the user.

- **Home time zone**

Home time zone of the user. The time zone set here is used to define the default Date and Time values for the user on the user interface of OpenScape UC Application.

- **Default language**

The language selected here defines for the user in which language the voice portal plays greetings after the user has logged in at the system.

- **Address translation context**

Address translation context used for normalizing and localizing phone numbers specific to users.

6) Switch to the **Password / PIN** tab and enter the following data:

- **Login password / Login password (confirm)**

User password.

The password must by default:

- comprise at least eight characters
- contain at least one capital letter
- contain at least one digit
- contain at least one special character
- contain each character not more than three times in succession

NOTICE: [Changing the User Passwords Policies](#) on page 572 describes how to change these password defaults.

- **Two Factor Authentication (2FA)**

NOTICE: To enable 2FA, you first need to configure the email address for the user (email1), as the 2FA code is sent via email.

- **Enable 2FA:** Check this checkbox to enable Two Factor Authentication.

- **Telephony PIN / Telephony PIN (confirm)** PIN for the assigned telephone.

The PIN must comprise eight to 16 digits by default.

NOTICE: [Changing Policies for User PINs](#) on page 576 describes how to change these PIN defaults.

7) Switch to the **Contact Information** tab and specify the required individual user information.

In doing so please heed the following:

- Specifying an address in the **IM Address** field is mandatory.

If you do not use Instant Messaging, you need to enter a dummy value – e. g. <user ID>@system

In case of Very Large Deployment a valid instant-messaging address must be specified for each OpenScape user – even if you do not use instant messaging. This address is required for inter-cluster communication.

NOTICE: The Instant Messaging address of a user is composed of the respective OpenScape user name (**Username**) and the domain name specified

upon the setup of the Openfire server. *Example:*
Monica.Sample@openfire.mycompany.com

- So that other OpenScape users can find the relevant user by searching the OpenScape user database, you need to fill in the **Last name** field at least.
 - Leave the **Business phone 1** field empty. The ONS number that you later configure on the **Resources** tab for the user is automatically entered here.
 - You need to consider whether to enter further phone numbers for the user. Other OpenScape users may call such numbers directly, thus avoiding the concept of the one-number service (ONS).
- 8) Switch to the **Profiles** tab.
- 9) In the **Assigned to user** column select the check boxes of the user profiles the privileges of which you would like to assign to the user.

As a rule, assign at least one user profile to each user account. We recommend not to assign default profiles to users since these profiles allow only a very insufficient privilege gradation. Instead, you should create and use individual user profiles for operating the OpenScape system. How to create new user profiles and edit them is described in the *OpenScape Common Management Platform, Administrator Documentation* manual.

NOTICE: Please refer to [User Privileges for OpenScape UC Application](#) on page 719 , Configuration and Administration manual to see which functions are assigned to the UC Application default profiles **Essential**, **Professional** and **Team** and to the CMP administrator profiles.

NOTICE: The license database of the OpenScape system may at times contain contradictory information for a profile. As a result, the license control of the OpenScape system may withdraw privileges from users with this profile though such privileges are displayed in the profile management for the relevant profile. How to correct such database inconsistencies is described in [Synchronizing License Assignments anew](#) on page 580.

- 10) Click on **Save** to copy the settings.
- 11) Create a user account for each OpenScape user in the same way or via the user management of the CMP.

You have now created all required user accounts.

NOTICE: A new user account is not operable in OpenScape UC Application until you have configured the one-number service for this account. You do that in [Configuring the One-number Service \(ONS\)](#) on page 151.

4.8 Configuring the One-number Service (ONS)

IMPORTANT: An OpenScape user can configure any terminal as his/her preferred device (OND). This enables him/her to accept or initiate calls via this device without direct physical access to it. If the relevant device is configured in a way that it automatically activates hands-free features in case of inbound and / or outbound calls, the OpenScape user can, for example, overhear the associated room without present persons noticing this. Therefore, deactivate the automatic activation of hands-free features for all terminals present in rooms where confident calls are made.

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

A user account is in OpenScape UC Application not operable until you have configured the one-number service for this account.

How to configure the one-number service:

- 1) [Configuring the ONS Number](#)
- 2) **For OpenScape Voice as communications system:**
[Activating the One-Number Service in OpenScape Voice](#)
- 3) **For OpenScape Voice as communications system:**
[Configuring the CTI Monitoring in OpenScape Voice](#)
- 4) **For OpenScape Voice as communications system:**
[Configuring an alternative Destination in OpenScape Voice](#)
- 5) [Configuring Device Settings](#)

These steps are described in detail in the following sections.

4.8.1 Configuring the ONS Number

So that an OpenScape user can deploy the one-number service, you need to assign this user his/her subscribers and configure one of these subscribers as ONS number.

Start the configuration

How to configure the ONS number for an OpenScape user:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain in which the relevant user account has been created.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Accounts > List**.

A list of all users configured in the selected domain appears in the workspace.

- 4) Click on the login name of the desired user.

The dialog with the settings of the relevant user opens.

- 5) Switch to the **Resources** tab.

All resources assigned to the user are displayed.

- 6) Click the **Advanced...** button.

A list of all subscribers who you can assign to the user appears.

- 7) Select the checkbox of the subscriber you want to assign to the user.

You can also assign several subscribers to a user. Doing that results in the following:

- The user can pick a subscriber as preferred device in his/her UC Application client.
- The conference portal uses the additional subscribers to identify a caller as OpenScape user.
- The additional subscribers influence the media presence status of the user if they belong to an OpenScape Voice or OpenScape 4000 system connected to OpenScape UC Application.

- 8) Click on **OK** to copy the selected subscriber for the user.

The newly copied subscriber is now displayed as phone number entry under **Number**.

- 9) Open the action menu of the phone number entry that you want to configure as ONS phone number for the user. To do this, click on  in the relevant list entry.

- 10) Select **Set as ONS number**.

The phone number is marked with  in the **Assigned** column as ONS number.

NOTICE: If a phone number is already monitored by a CSTA application, it must not be configured as ONS phone number. This refers e.g. to phone numbers already monitored by ComAssistant or OpenScape Contact Center.

NOTICE: No matter which name you assign to the ONS number in the CMP: The UC Application clients will always display this number with the name **Office Phone**. The

name assigned to the ONS number in the CMP will not be put out in the domain export file either.

- 11) Click on **Save** to copy the settings.

You have now configured the ONS number for the OpenScape user.

Configuring several SIP subscribers for one user at OpenScape Voice

If you want to use a desk phone and a soft client as SIP subscribers at OpenScape Voice for one user, proceed as follows:

- Configure different phone numbers for both SIP subscribers in OpenScape Voice.
- Assign the desk phone number to the user as ONS number.
- Assign the soft client number to the user as additional resource.

4.8.2 Activating the One-Number Service in OpenScape Voice

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice as communications system.

So that an OpenScape user can deploy the one-number service at OpenScape Voice, you need to activate this service in the settings of all of his/her OpenScape Voice subscribers and perform an additional setting.

Start the configuration

How to activate the one-number service in the settings of an OpenScape Voice subscriber:

- 1) On the **Configuration** navigation tab of the CMP click on the **OpenScape Voice** navigation menu item.
- 2) In the navigation tree, click on Business Group.
- 3) Select the business group in which the subscriber is configured from the Business Group combo box.
- 4) Click on **Members > Subscribers**.
A list of all subscribers configured in the selected business group appears in the work area.
- 5) Click on the **Directory Number** of the desired subscriber.
The dialog with the settings of the relevant subscriber opens.
- 6) Switch to the **Features** tab.
- 7) Activate the **One Number** service.
- 8) Click on the service name **One Number** to display the settings of the service.
The configuration dialog of the service opens.
- 9) Select under **One Number Service status** the **Inbound and Outbound** option.
- 10) Select **OK**.
- 11) Switch to the **Displays** tab.

- 12) Enter under **External Caller ID** the ONS number of the relevant user.

NOTICE: This telephone number is displayed to external callees if the one-number service of OpenScape UC Application fails. This setting is particularly important if the respective user deploys a soft phone for outgoing calls and in OpenScape Voice this soft phone is not assigned a telephone number that can actually be dialed.

- 13) Select **Save**.
- 14) Execute the described steps for all OpenScape Voice subscribers assigned to OpenScape users.

You have now configured the one-number service in the OpenScape Voice subscriber settings.

4.8.3 Configuring the CTI Monitoring in OpenScape Voice

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice as communications system.

Before an OpenScape user can deploy the one-number service, CTI monitoring must be activated in OpenScape Voice for all subscribers of the user.

Start the configuration

Activate the CTI monitoring for a subscriber by continuing in the subscriber's settings as follows:

- 1) Check that the **Features** tab is displayed.
- 2) Activate the **CSTA Access** service.
- 3) Click on the service name **CSTA Access** to display the settings of the service.

The configuration dialog of the service opens.

- 4) Select one of the following options under **CSTA Type**:
 - **CSTA over SIP** if the subscriber uses an OpenStage device.
 - **Type 1**⁶ if the subscriber uses an OptiPoint or the OpenScape Web Client as a softphone.
- 5) Execute the described steps for all OpenScape Voice subscribers assigned to OpenScape users.
- 6) Select **OK**.

You have now activated the CTI monitoring in the subscriber settings of OpenScape Voice.

⁶ In earlier OpenScape Voice versions this option is called **Siemens Type 1**.

4.8.4 Configuring an alternative Destination in OpenScape Voice

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice as communications system.

You must configure an alternative target for subscribers who use the one-number service. If the one-number routing fails for some reason, this alternative destination ensures that incoming calls are routed to a specified device.

Start the configuration

Configure an alternative target for a subscriber by executing the steps of the following guide:

- 1) Add the feature **Call Forwarding – Dependable** for the subscriber.
- 2) Enable the **Activate** option in the feature settings.
- 3) In the feature settings, specify under **Redirect Number – Internal** and **Redirect Number – External** the directory number of the subscriber who shall act as routing destination if the one-number routing of OpenScape UC Application is disturbed.

You have now configured a dependable routing for the OpenScape Voice subscriber.

4.8.5 Configuring Device Settings

To enable OpenScape users deploying the one-number service in combination with their terminal device, you need to perform various settings for such users in the communications system used.

If you fail to do so, the one-number service cannot control the terminal devices properly when OpenScape users deploy the consultation or toggle function in their OpenScape client.

The necessary settings vary depending on the type of device used.

- [OptiPoint Devices and OpenScape Desktop Client](#)
- [OpenStage Device](#)

4.8.5.1 OptiPoint Devices and OpenScape Desktop Client

How to configure OptiPoint devices and the OpenScape Desktop Client for using the one-number service:

- 1) Activate the **Auto answer** option in the device settings.
- 2) Activate the **Auto reconnect** option in the device settings.

4.8.5.2 OpenStage Device

How to configure OpenStage devices for using the one-number service:

- 1) Activate the **CTI Autoanswer** option in the device settings.

- 2) Activate the **CTI Reconnect** option in the device settings.
- 3) Activate the **uaCSTA** option in the device settings.

You have now fully configured the one-number service.

All users for whom you have configured the one-number service are now operable for OpenScape UC Application.

4.9 Configuring the Conference Portal

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

How to configure the conference portal:

- 1) **If you do not use several Media Servers operating in parallel:**
[Configuring the Conference Portal Acces](#)
- 2) **If you do not use several Media Servers operating in parallel:**
[Configuring a CTI Connection](#)
- 3) [Configuring the Conference Component](#)
- 4) [Configuring the Phone Number Normalization](#)
- 5) **If you use video conferences of the conference portal:**
[Activating RTCP for Video Conferences](#)
- 6) **If you use several Media Servers operating in parallel:**
[Configuring the Conference Portal for Media Server Farm](#)
- 7) If you use Integrated Deployment with External Media Server: [Configuring the Conference Portal for Integrated Deployment with External Media Server for Video Conferences](#)
- 8) If you do not connect to a groupware system:
[Configuring the SMTP Server Connection](#)
- 9) **If you use video conferences of the conference portal:**
[Configuring Video Systems](#)

These steps are described in detail in the following sections.

4.9.1 Configuring the Conference Portal Acces

NOTICE: If you use several Media Servers operating in parallel, skip this chapter: Configuring such a Media Server farm is described in [Configuring the Conference Portal for Media Server Farm](#) on page 163.

The conference portal must be available via an individual access number.

Start the configuration

How to configure the conference portal access number:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) Switch to the Configuration tab.
- 4) Select **Bridge numbers** under Number Configuration.
- 5) Click Add to specify the phone number you wish to use as access number for the conference portal.

This setting defines the phone number used as originator address when the conference portal initiates a call or sends an e-mail.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

- 6) Click on **OK**.
- 7) Switch to the Trunk numbers tab and select the corresponding media server node.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

IMPORTANT: The field Trunk Number must not be empty, else problems with Conferences could appear.

- 8) Under the **Media Server node configuration** tab, verify that the **Trunk number** field displays the bridge number you just entered under **Bridge numbers**.
- 9) Click on **Save** to copy the access number for the conference portal in the relevant OpenScape Media Server.
- 10) Switch to the **Configuration** tab in the conference dialog of the conference portal plug-in.
- 11) Select **Default language** under Media configuration in order to set the language to be used as default for accessing the conference portal.

NOTICE: The default language setting does not affect callers who can be uniquely identified as OpenScape users. It applies exclusively for users who cannot be uniquely identified as OpenScape users.

- 12) Click on **Save** to apply the changed settings.

NOTICE: To provide conference portal access for further default languages you need to configure an additional conference portal access for every additionally desired default language. Proceed as described in [Configuring the](#)

[Conference Portal Access for another existing Language](#) on page 469.

You have now configured the access number for the conference portal.

4.9.2 Configuring a CTI Connection

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. The configuration of such a Media Server farm is described in [Configuring the Conference Portal for Media Server Farm](#) on page 163 and will refer to this section in due course.

The BCom provider of OpenScape UC Application and the OpenScape Media Server need to intercommunicate via CTI messages for signaling conference connections. A CTI connection must be configured between these two systems for this purpose.

Start the configuration

How to configure a CTI connection between the BCom provider and the OpenScape Media Server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Media Server**.

The workspace shows all configured CTI connections of the Media Servers.

- 3) Select **Add** to create a new CTI connection to a Media Server.
The configuration dialog for creating a new CTI connection opens.
- 4) In the **Media Server** field select the server on which you have previously configured the conference portal. Cf. [Configuring the Conference Portal Access](#) on page 156.

NOTICE: For each Media Server only one connection can be configured. If no Media Server can be selected in the **Media Server** field, a CSTA connection is already configured for each Media Server.

- 5) In the **Version** field select the **Global Number Format (GNF)** entry.
- 6) Select **Add** to create a new CTI connection for the Media Server.
The configuration dialog for creating a new CTI connection opens.
- 7) Specify in the **Connection Name** field a name for the new CTI connection.
Under this name the CTI connection will later be administered in the CMP.
- 8) Select one of the available entries in the **BCom Provider** field.
- 9) Select **OK** to copy the settings of the new CTI connection.
The new CTI connection is now displayed to you in the list of CTI connections.
- 10) Select **Save** to copy the settings.

You have now configured the CTI connection between OpenScape Media Server and the BCom Provider of OpenScape UC Application.

4.9.3 Configuring the Conference Component

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. The configuration of such a Media Server farm is described in [Configuring the Conference Portal for Media Server Farm](#) on page 163 and will refer to this section in due course.

NOTICE: The maximum number of conference participants is restricted to 200. In Trunk Number settings you can not set a maximum participants number larger than 200..

You can perform different settings for the conference portal. You perform such settings in the conference component.

Start the configuration

How to configure the most important settings of the conference component:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Conferences**.
The configuration dialog of the conference portal plugin opens.
- 3) Switch to the Configuration tab.
- 4) Under Number configuration, select **Bridge numbers**.
- 5) If required, specify an access number via which the conference portal can be reached free of charge, by clicking Add and entering all required details.

The specified phone number is displayed in OpenScape clients and in e-mails that the conference portal sends.

- 6) If required, specify further access numbers via which the conference portal can be reached. Switch to the Trunk Numbers tab, select the media server node and configure the additional numbers under Additional numbers. If you want to specify several phone numbers, separate them by a semicolon followed by a blank.

Example: German: +49 2440 901100; English: +49 2440 901200

The specified phone numbers are displayed in OpenScape clients and in e-mails that the conference portal sends.

- 7) Switch to the **Conference settings** tab.
- 8) How to have conferences prolonged automatically:
 - a) Specify under **Duration (in minutes)** the maximum duration of an automatically prolonged conference.

If a conference's duration reaches the value specified here, it cannot be automatically prolonged any further. If a prolonged duration has already been defaulted at the conference start, this prolonged conference duration applies. Such a conference is generally not automatically prolonged though.

- b) Select the **Auto-Prolong On** option for prolonging conferences automatically.

Conferences can be automatically prolonged when the end of the scheduled conference duration is reached but conference participants are still logged in. Appropriate portal resources must be available for a conference to be prolonged.

- c) Specify under **Prolong time (in minutes)** the extra time to be added to a conference.
- 9) How to perform the settings for the conference portal's internal maintenance works:
- a) Set under **Time** a weekday or Daily/Hourly to specify for the conference component the frequency of starting its maintenance works automatically.

NOTICE: During maintenance work, reservations of unused conferences are deleted.

- b) Select under **at** the precise time for the conference component to start its maintenance works automatically. The following applies:

- If you select a weekday or Daily under **Time** you need to specify an hour in the format <hh>:<mm> under **at**. This is then the hour at which maintenance works start on the selected day.
- If you select **Hourly** under **Time** you need to specify minutes in the format <mm> under **at**. This is then the minute at which maintenance works start every hour.

- 10) Switch to the **Configuration** > Configuration Settings.
- 11) Select **Timer settings**.

The **Timer settings** configuration dialog opens.

- 12) Specify under **Conference forerun period** the grace period for starting a conference.

As a rule the clocks of the conference participants are not harmonized. This may lead to some participants logging on to the conference portal shortly before the conference actually starts. But because the conference has actually not started yet, they receive a corresponding information, are rejected and need to log on at a later date.

Via **Conference forerun period** you can start any conference some specified time before the actual conference start. Conference participants who dial in can thus enter the conference room earlier.

NOTICE: Conference forerun period does not influence the time when conference participants are called by the conference portal to join the conference.

- 13) Specify under **Conference grace period** the grace period for terminating a conference.

If a criterion for ending a conference occurs, there is still the configured grace period for the conference to stay active. The conference is not

definitely terminated until the grace period has expired and the criterion for ending the conference is still valid.

NOTICE: Criteria for ending a conference: The last user logs off (open conference), the last moderator logs off (moderated conference).

- 14) Specify under **Call-out ring timeout** the time the conference component shall wait for a callee to accept an automatically initiated call.

If the callee does not answer the phone within this period, the conference component stops calling and does not make any further attempts to initiate this call either.

- 15) Select **Save** to copy the changed time profile settings.

- 16) Select **Save** to copy the changed settings.

You have now performed the most important settings of the conference component.

4.9.4 Configuring the Phone Number Normalization

After a caller has logged in to the conference portal, the conference portal tries to identify the caller as an OpenScape user. To do this, it searches the OpenScape user database for a user to whom the originator number used has been assigned as a number resource in CMP.

To compare the originator number used to the number resources, the conference portal needs to convert the originator number to a normalized number format before. The conference portal needs a so-called address translation context.

Start the configuration

How to define the address translation context for the conference portal:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) Click on Configuration tab.
- 4) Select under Configuration the Configuration Settings tab.
- 5) Select under **Address translation context** the address translation context the conference portal shall use for normalizing phone numbers.

NOTICE: This address translation context must have previously been configured in the CMP. Compare [Configuring Address Translation Contexts](#) on page 140.

- 6) Select **Save** to copy the new settings.

You have now configured the phone number normalization for the conference portal.

4.9.5 Activating RTCP for Video Conferences

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. The configuration of such a Media Server farm is described in [Configuring the Conference Portal for Media Server Farm](#) on page 163 and will refer to this section in due course.

NOTICE: You need to execute the configuration steps of this chapter only if you use Lifesize systems for the video conferences of the conference portal.

You need to activate the RTCP protocol in the OpenScape Media Server for evading a software bug in the firmware of video systems by Lifesize.

Start the configuration

How to activate RTCP in the OpenScape Media Server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.
You see a list of all Media Servers available in the OpenScape system.
- 3) Click on the name of the desired OpenScape Media Server.
The configuration dialog of the selected OpenScape Media Server opens.
- 4) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.
- 5) In the provider list select the link **Streaming (RTP)**.
The configuration dialog with the streaming provider settings opens.
- 6) Select in the list of configured RTP streaming routes the radio button of the RTP streaming route used for the conference portal.
This is by default the RTP streaming route with the ID **default**.
- 7) Select **Edit**.
The configuration dialog for the selected RTP streaming route opens.
- 8) Select the **RTCP Reporting**.
- 9) Select **Save** to copy the setting.
- 10) If you use further RTP streaming routes for the conference portal, configure RTCP for these routes as well.
- 11) Select **Close**.
- 12) Verify that the **Streaming (RTP)** radio button of the provider is enabled on the **Providers** tab of the configuration dialog.
- 13) Select **Restart Provider**.

You have now activated RTCP for video conferencing.

4.9.6 Configuring the Conference Portal for Media Server Farm

NOTICE: You need to execute the configuration steps of this chapter only if you use several Media Server servers operating in parallel.

NOTICE: A description of how the conference portal uses the configuration outlined in the following is provided by the *OpenScape Media Server, Administrator Documentation* manual in the Media Server farm context.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

NOTICE: The numbering scheme used in this chapter is merely an example to illustrate the correlations in the system configuration. You can also choose an approach similar to this numbering scheme but better suited for the available system environment.

You can use OpenScape UC Application with several OpenScape Media Servers operating in parallel – a so-called Media Server farm.

Start the configuration

Configure the conference portals of the different OpenScape Media Servers for a Media Server farm by following the steps of the following guide.

- 1) Configure in OpenScape Voice a new endpoint in the global numbering plan for each OpenScape Media Server of the Media Server farm.
 - a) Select on the **SIP** tab type **Static** for each endpoint..
 - b) Specify the IP address of the respective OpenScape Media Server in the **Endpoint Address** field.
 - c) Switch to the **General** tab and activate for each endpoint the **Registered** option.
 - d) Switch to the **Attributes** tab and activate the **Allow Sending of Insecure Referred-By Headers** option.
 - e) Switch to the **Attributes** tab and activate the **Send International Numbers in Global Number Format (GNF)** option. OpenScape Voice then sends all GNF-based phone numbers with a leading + character to the OpenScape Media Server.

Example of a Media Server farm with two OpenScape Media Servers:

	Endpoint 1	Endpoint 2
Endpoint name:	EP_MS-1	EP_MS-2

	Endpoint 1	Endpoint 2
Endpoint IP address:	10.1.1.21	10.1.1.22

NOTICE: You can use these endpoints for the voice as well as for the conference portal of a Media Server farm.

- 2) Configure a new shared destination in the global numbering plan in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

Example: DEST_MS-ALL

- 3) Create in the shared destination a route to each of the OpenScape Media Servers.
 - a) Assign an individual ID to each route.
 - b) In doing so, select the **SIP Endpoint** option for **Endpoint Type**.
 - c) Select under **SIP Endpoint** the endpoint of the respective OpenScape Media Server.
 - d) Select under **Modification Type** the **Number Manipulation** option. Select under **Nature of Address** the **International** option.

Example of a Media Server farm with two OpenScape Media Servers:

Destination:	Routes	
DEST_MS-ALL	Route 1	Route 2
ID:	1	2
SIP Endpoint:	EP_MS-1	EP_MS-2

NOTICE: You can use this shared destination for the voice as well as for the conference portal of a Media Server farm.

- 4) Configure an individual new destination in the global numbering plan in OpenScape Voice for each OpenScape Media Server of the Media Server farm.
- 5) Create in the respective destination a route to the relevant OpenScape Media Server.
 - a) Assign an individual ID to each route.
 - b) In doing so, select the **SIP Endpoint** option for **Endpoint Type**.
 - c) Select under **SIP Endpoint** the endpoint of the respective OpenScape Media Server.
 - d) Select under **Modification Type** the **Number Manipulation** option.
 - e) Select under **Nature of Address** the **International** option.

Example of a Media Server farm with two OpenScape Media Servers:

Destination:	Routes	
DEST_MS-1	Route	
ID:	1	

Destination:	Routes	
DEST_MS-1	Route	
SIP Endpoint:	EP_MS-1	

Destination:	Routes	
DEST_MS-2		Route
ID:		2
SIP Endpoint:		EP_MS-2

- 6) Configure a shared prefix access code in the global numbering plan in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

Callers will be able to reach the conference portal of all OpenScape Media Servers under this prefix access code.

Use the following format for the prefix access code:

<GNF Prefix Replacement><Country Code><Area Code><Local Office Code><Extension "minus one digit">

Example: 0004924040901120

The following applies:

<i><GNF Prefix Replacement></i>	:	000
<i><Country Code></i>	:	49
<i><Area Code></i>	:	240
<i><Local Office Code></i>	:	40901
<i><Extension></i>	:	1200

For this example, enter digit 3 under **Digit Position** to cut the leading digit sequence **000**. This will ensure that the phone number matches the destination code to be configured at a later date.

NOTICE: You can use this shared prefix access code for the voice as well as for the conference portal of a Media Server farm.

- 7) Configure an individual prefix access code in the global numbering plan in OpenScape Voice for each OpenScape Media Server of the Media Server farm.

These prefix access codes are used for the internal communication of the OpenScape Media Servers with each other.

Use for the individual prefix access codes the same format as for the shared prefix access code.

Example of a Media Server farm with two OpenScape Media Servers:

	shared	Media Server 1	Media Server 2
Prefix access code	0004924040901120	0004924040901121	0004924040901122

For this example, enter digit 3 under **Digit Position** to cut the leading digit sequence **000**. This will ensure that the phone number matches the destination code to be configured at a later date.

- 8) Configure a shared destination code in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

The conference portal of all OpenScape Media Servers will be accessible under this destination code.

In doing so, select the shared destination of all OpenScape Media Servers under **Destination Name**.

Use for example the following format for the destination code:

<Country Code><Area Code><Local Office Code><Extension “minus one digit”>

Example: 4924040901120

NOTICE: You can use this shared destination code for the voice as well as for the conference portal of a Media Server farm.

- 9) Configure an individual destination code in OpenScape Voice for each OpenScape Media Server of the Media Server farm.

These destination codes are used for the internal communication of the OpenScape Media Servers with each other.

In doing so, select the destination of the respective OpenScape Media Server under **Destination Name**.

Use for the individual destination codes the same format as for the shared destination code.

Example of a Media Server farm with two OpenScape Media Servers:

	shared	Media Server 1	Media Server 2
Prefix access code	0004924040901120	0004924040901121	0004924040901122

	shared	Media Server 1	Media Server 2
Destination code	4924040901120 with the destination: DEST_MS-ALL	4924040901121 with the destination: DEST_MS-1	4924040901122 with the destination: DEST_MS-2

- 10) If the endpoints of the OpenScape Media Servers and the OpenScape Voice subscribers are configured under different numbering plans, you must configure comparable destinations, routes, prefix access codes and destination codes for all involved numbering plans.

This applies e. g. if the OpenScape Voice subscribers are configured under a private numbering plan and the OpenScape Media Server endpoints under E.164.

- 11) Configure a common phone number for the conference portal access that uses English as default language on each OpenScape Media Server of the Media Server farm as follows.

Users may later dial into the conference portal under this number with the TUI being played in English to user who do not deploy OpenScape.

a) Click on the **Unified Communications** tab.

b) In the navigation tree, click on **Configuration > Conferences**

The configuration dialog of the conference portal plugin opens

c) Verify that Configuration tab is displayed.

d) Click on **Trunk numbers**.

e) Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

f) Check that the **Media Server node configuration** tab is displayed.

g) Specify under **New number** the phone number you wish to use as shared phone number for the English-language conference portal access.

In doing so please consider the shared destination code you configured in step 8.

h) Select the **Create on all nodes** option.

i) Select **Add**.

The newly configured phone number is added to the phone number list. The **Create on all nodes** column features **Yes**.

Example of a Media Server farm with two OpenScape Media Servers and the example destination code from step 8:

	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201

j) Select **Save** to create the shared phone number for conference portal access on all OpenScape Media Servers.

- 12) To provide conference portal access for other default languages also, configure another common phone number for each additionally required

default language on each OpenScape Media Server of the Media Server farm as follows.

- a) Click on the **Unified Communications** tab.
- b) In the navigation tree, click on **Configuration > Conferences**. The configuration dialog of the conference portal plugin opens.
- c) Verify that Configuration tab is displayed.
- d) Click on **Lang. dep. bridge numbers**.

The dialog for configuring language dependent bridge numbers opens.

- e) Select **Language dependent bridge numbers**.

The dialog for configuring language dependent bridge numbers opens.

- f) Specify under **New number** the phone number for reaching the conference portal access of the additional default language.

In doing so consider the destination code you configured in step 8.

- g) Select the language the conference portal access shall use as default language from the associated combo box.
- h) Select **Add**.

The new bridge number is added to the list of bridge numbers.

- i) Select **Save** to create the newly added bridge number on all OpenScape Media Servers.

The newly added bridge number is added to all OpenScape Media Servers of the Media Server farm.

Example of a Media Server farm with two OpenScape Media Servers and the example destination code from step 8:

	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201
Common phone number of the portal access (e. g. for German):	49240409011202	49240409011202
Common phone number of the portal access (e. g. for Chinese):	49240409011203	49240409011203

- 13) Configure another phone number specific to the Media Server for accessing the conference portal on each OpenScape Media Server of the Media Server farm as follows.

These phone numbers will later be required by the OpenScape Media Servers for the internal routing within the Media Server farm. They are independent from the default language.

- a) Click on the **Unified Communications** tab.
- b) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- c) Verify that Configuration tab is displayed.
- d) Click on **Trunk numbers**.
- e) Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f) Check that the **Media Server node configuration** tab is displayed.
- g) Specify under **Trunk number** the phone number you wish to use as individual phone number for the conference portal access of this OpenScape Media Server.

In doing so consider the destination code you configured in step 8.

- h) Click on **Save** to copy the access number for the conference portal in the relevant OpenScape Media Server.
- i) Execute the described steps for each OpenScape Media Server of the Media Server farm.

Example of a Media Server farm with two OpenScape Media Servers and the example destination code from step 8:

OpenScape Media Server	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201
Common phone number of the portal access (e. g. for German):	49240409011202	49240409011202
Common phone number of the portal access (e. g. for Chinese):	49240409011203	49240409011203
Individual phone number of the portal access (for all languages):	49240409011210	49240409011220

- 14) Configure the CTI link for each OpenScape Media Server of the Media Server farm. Proceed as described in [Configuring a CTI Connection](#) on page 158.
- 15) Configure a uniform bridge number for each conference portal of the different OpenScape Media Servers. Proceed as described in [Configuring the Conference Component](#) on page 159.

- 16) If you use Lifesize systems for the video conferences of the conference portal, activate RTCP for each OpenScape Media Server. Proceed as described in [Activating RTCP for Video Conferences](#) on page 162.

After this configuration the conference portal solution is now operable for a Media Server farm.

4.9.7 Configuring the Conference Portal for Integrated Deployment with External Media Server for Video Conferences

You can use an integrated deployment of the OpenScape UC Application with an external media server operating in parallel, in order to support video conference capabilities. Video streaming must be configured on the external media server.

NOTICE: You need to execute the configuration steps of this chapter only if you use integrated deployment server with external media server for video conferences operating in parallel.

NOTICE: A description of how the conference portal uses the configuration outlined in the following is provided by the *OpenScape Media Server, Administrator Documentation* manual in the context of Integrated Deployment Server with External Media Server for Video Conferences.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

NOTICE: The numbering scheme used in this chapter is merely an example to illustrate the correlations in the system configuration. You can also choose an approach similar to this numbering scheme but better suited for the available system environment.

Start the configuration

Configure the conference portals of the different OpenScape Media Servers for an Integrated Deployment with External Media Server by following the steps below.

- 1) Configure in OpenScape Voice a new endpoint in the global numbering plan for both the integrated deployment media server and the external media server.
 - a) Select on the **SIP** tab type **Static** for each endpoint.
 - b) Specify the IP address of the respective OpenScape Media Server in the **Endpoint Address** field.
 - c) Switch to the **General** tab and activate for each endpoint the **Registered** option.
 - d) Switch to the **Attributes** tab and activate the **Allow Sending of Insecure Referred-By Headers** option.
 - e) Switch to the **Attributes** tab and activate the **Send International Numbers in Global Number Format (GNF)** option. OpenScape Voice then sends all GNF-based phone numbers with a leading + character to the OpenScape Media Server.

Example of an integrated deployment server with an external media server:

	Endpoint 1 (integrated MS)	Endpoint 2 (external MS)
Endpoint name:	EP_MS-1	EP_MS-2
Endpoint IP address:	10.1.1.21	10.1.1.22

NOTICE: You can use this shared destination for the voice as well as for the conference portal of an integrated deployment with an external media server.

NOTICE: The external media server will be used to stream video conferences.

- 2) Configure a new shared destination in the global numbering plan in OpenScape Voice for all both integrated and external OpenScape Media Servers.

Example: DEST_MS-ALL

- 3) Create in the shared destination a route to each of the OpenScape Media Servers.
 - a) Assign an individual ID to each route.
 - b) Select the **SIP Endpoint** option for **Endpoint Type**.
 - c) Select under **SIP Endpoint** the endpoint of the respective OpenScape Media Server.
 - d) Select under **Modification Type** the **Number Manipulation** option.
 - e) Select under **Nature of Address** the **International** option.

Example of an integrated deployment server with an external media server:

Destination:	Routes	
DEST_MS-ALL	Route 1	Route 2
ID:	1	2

Destination:	Routes	
DEST_MS-ALL	Route 1	Route 2
SIP Endpoint:	EP_MS-1	EP_MS-2

NOTICE: You can use this shared destination for the voice as well as for the conference portal of an integrated deployment with an external media server.

- 4) Configure an individual new destination in the global numbering plan in OpenScape Voice for each OpenScape Media Server.
- 5) Create in the respective destination a route to the relevant OpenScape Media Server.
 - a) Assign an individual ID to each route.
 - b) Select the **SIP Endpoint** option for **Endpoint Type**.
 - c) Select under **SIP Endpoint** the endpoint of the respective OpenScape Media Server.
 - d) Under **Modification Type**, select the **Number Manipulation** option.
 - e) Under **Nature of Address**, select the **International** option.

Example of an integrated deployment server with an external media server:

Destination:	Routes	
DEST_MS-1	Route	
ID:	1	
SIP Endpoint:	EP_MS-1	

Destination:	Routes	
DEST_MS-2		Route
ID:		2
SIP Endpoint:		EP_MS-2

- 6) Configure a shared prefix access code in the global numbering plan in OpenScape Voice for both OpenScape Media Servers.

Callers will be able to reach the conference portal of all OpenScape Media Servers under this prefix access code.

Use the following format for the prefix access code:

<GNF Prefix Replacement><Country Code><Area Code>
><Local Office Code><Extension "minus one digit">

Example: 0004924040901120

The following applies:

<GNF Prefix Replacement>	:	000
<Country Code>	:	49

<Area Code >	:	240
<Local Office Code >	:	40901
<Extension >	:	1200

For this example, enter digit 3 under **Digit Position** to cut the leading digit sequence **000**. This will ensure that the phone number matches the destination code to be configured at a later date.

NOTICE: You can use this shared prefix access code for the voice as well as for the conference portal of an integrated deployment with external server.

- 7) Configure an individual prefix access code in the global numbering plan in OpenScape Voice for each OpenScape Media Server.

These prefix access codes are used for the internal communication of the OpenScape Media Servers with each other.

Use for the individual prefix access codes the same format as for the shared prefix access code.

Example of an integrated deployment server with an external media server:

	shared	Media Server 1	Media Server 2
Prefix access code	0004924040901120	0004924040901121	0004924040901122

For this example, enter digit 3 under **Digit Position** to cut the leading digit sequence **000**. This will ensure that the phone number matches the destination code to be configured at a later date.

- 8) Configure a shared destination code in OpenScape Voice for both OpenScape Media Servers.

The conference portal of both OpenScape Media Servers will be accessible under this destination code.

In doing so, select the shared destination of both OpenScape Media - Servers under **Destination Name**.

Use for example the following format for the destination code:

<Country Code><Area Code><Local Office Code><Extension "minus one digit">

Example: 4924040901120

NOTICE: You can use this shared destination code for the voice as well as for the conference portal of an integrated deployment with external server.

- 9) Configure an individual destination code in OpenScape Voice for each OpenScape Media Server.

These destination codes are used for the internal communication of the OpenScape Media Servers with each other.

Select the destination of the respective OpenScape Media Server under **Destination Name**.

Use for the individual destination codes the same format as for the shared destination code.

Example of a Media Server farm with two OpenScape Media Servers:

	shared	Media Server 1	Media Server 2
Prefix access code	0004924040901120	0004924040901121	0004924040901122
Destination code	4924040901120	4924040901121	4924040901122
	with the destination: DEST_MS-ALL	with the destination: DEST_MS-1	with the destination: DEST_MS-2

- 10) If the endpoints of the OpenScape Media Servers and the OpenScape Voice subscribers are configured under different numbering plans, you must configure comparable destinations, routes, prefix access codes and destination codes for all involved numbering plans.

This applies e. g. if the OpenScape Voice subscribers are configured under a private numbering plan and the OpenScape Media Server endpoints under E.164.

- 11) Configure a common phone number for the conference portal access that uses English as default language on each OpenScape Media Server as follows.

Users who do not deploy OpenScape may later dial into the conference portal under this number with the TUI being played in English.

- a) Click on the **Unified Communications** tab.
- b) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- c) Verify that Configuration tab is displayed.
- d) Click on **Trunk numbers**.

IMPORTANT: The field Trunk Number must not be empty, else problems with Conferences could appear.

- e) Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f) Check that the **Media Server node configuration** tab is displayed.
- g) Specify under **New number** the phone number you wish to use as shared phone number for the English language conference portal access.

In doing so please consider the shared destination code you configured in step 8.

- h) Select the **Create on all nodes** option.
- i) Select **Add**.

The newly configured phone number is added to the phone number list. The **Create on all nodes** column features **Yes**.

Example of two OpenScape Media Servers (an integrated deployment with external server) and the example destination code from step 8:

	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201

- j) Select **Save** to create the shared phone number for conference portal access on all OpenScape Media Servers.

- 12) To provide conference portal access for other default languages also, configure another common phone number for each additionally required default language on each OpenScape Media Server as follows.

- a) Click on the **Unified Communications** tab.
- b) in the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- c) Verify that Configuration tab is displayed.
- d) Click on **Lang. dep. bridge numbers**.
- e) Click **Language dependent bridge numbers tab**.

The dialog for configuring language dependent bridge numbers opens.

- f) Specify under **New number** the phone number for reaching the conference portal access of the additional default language.

In doing so consider the destination code you configured in step 8.

- g) Select the language the conference portal access shall use as default language from the associated combo box.
- h) Select **Update**.

The new bridge number is added to the list of bridge numbers.

- i) Select **Save** to create the newly added bridge number on all OpenScape Media Servers.

The newly added bridge number is added to all OpenScape Media Servers.

Example of two OpenScape Media Servers (an integrated deployment with external server) and the example destination code from step 8:

	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201
Common phone number of the portal access (e. g. for German):	49240409011202	49240409011202
Common phone number of the portal access (e. g. for Chinese):	49240409011203	49240409011203

- 13)** Configure another phone number specific to the Media Server for accessing the conference portal on each OpenScape Media Server.

These phone numbers will later be required by the OpenScape Media Servers for the internal routing among them. They are independent from the default language.

- a)** Click on the **Unified Communications** tab.
- b)** Under Configuration in the navigation tree, click **Conferences**.

The configuration dialog of the conference portal plugin opens.

- c)** Verify that Configuration tab is displayed.
- d)** Click on **Trunk numbers**.
- e)** Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f)** Check that the **Media Server node configuration** tab is displayed.
- g)** Specify under **Trunk number** the phone number you wish to use as individual phone number for the conference portal access of this OpenScape Media Server.

In doing so consider the destination code you configured in step 8.

- h)** Click on **Save** to copy the access number for the conference portal in the relevant OpenScape Media Server.
- i)** Execute the described steps for each OpenScape Media Server.

Example of two OpenScape Media Servers (an integrated deployment with external server) and the example destination code from step 8:

OpenScape Media Server	Media Server 1	Media Server 2
Common phone number of the portal access (for English):	49240409011201	49240409011201
Common phone number of the portal access (e. g. for German):	49240409011202	49240409011202
Common phone number of the portal access (e. g. for Chinese):	49240409011203	49240409011203
Individual phone number of the portal access (for all languages):	49240409011210	49240409011220

- 14)** Configure the CTI link for each OpenScape Media Server. Proceed as described in [Configuring a CTI Connection](#) on page 158.
- 15)** Configure a uniform bridge number for each conference portal of the different OpenScape Media Servers. Proceed as described in [Configuring the Conference Component](#) on page 159.

16) Enable video on the external media server conferencing terminals:

- a)** Click on the **Unified Communications** tab.
- b)** Under Configuration in the navigation tree, click **Conferences**.
The configuration dialog of the conference portal plugin opens.
- c)** Verify that Configuration tab is displayed.
- d)** Click on **Trunk numbers**.
- e)** Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f)** Check that tab Media Server selection exists.
- g)** Under Media Type, enable video by clicking on the radio button next to video.
- h)** Click Save.

17) Deactivate video on the integrated deployment media server node:

- a)** Click on the **Unified Communications** tab.
- b)** Under Configuration in the navigation tree, click **Conferences**.
The configuration dialog of the conference portal plugin opens.
- c)** Verify that Configuration tab is displayed.
- d)** Click on **Trunk numbers**.
- e)** Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f)** Check that tab Media Server selection exists.
- g)** Under the Media Server selection tab> Media support, check Audio only. The Video check box must be unchecked.
- h)** Click Save.

18) Activate video on the external media server node:

- a)** Click on the **Unified Communications** tab.
- b)** Under Configuration in the navigation tree, click **Conferences**.
The configuration dialog of the conference portal plugin opens.
- c)** Verify that Configuration tab is displayed.
- d)** Click on **Trunk numbers**.
- e)** Click on the link of one of the displayed OpenScape Media Servers in the Media Server list.

The configuration dialog for the conference portal of the relevant OpenScape Media Server opens.

- f)** Check that tab Media Server selection exists.
- g)** Under the Media Server selection tab> Media support, check Video. The Audio only check box must be unchecked.
- h)** Click Save.

19) If you use Lifesize systems for the video conferences of the conference portal, activate RTCP for each OpenScape Media Server. Proceed as described in [Activating RTCP for Video Conferences](#) on page 162.

After this configuration the conference portal solution is now operable for an integrated deployment with external media server for video conferences.

4.9.8 Configuring the SMTP Server Connection

NOTICE: You need to execute the configuration steps of this chapter only if you do not connect a groupware system OpenScape UC Application.

NOTICE: Using the groupware-independent SMTP server connection requires installing the RPM package `gwbeshared`. How to proceed is described in the manual *OpenScape UC Application, Installation and Upgrade*.

If OpenScape UC Application is operated without an external groupware system, OpenScape UC Application must be connected with an external SMTP server. OpenScape UC Application sends all automatically generated e-mails via this connection – for example e-mails that invite for conferences.

Start the configuration

How to configure the connection to an SMTP server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

A window opens displaying all configured groupware connections.

- 3) Select **Add**.

The dialog for adding a new groupware connection opens.

- 4) The entry **SMTP** is automatically selected under **Connection Type**.
- 5) Specify a unique identifier for the connection under **Connection ID**.

Example: SMTP

- 6) Select **Save**.

The new connection is displayed in the list of all configured groupware connections.

- 7) Select the radio button of the connection you have just added.
- 8) Select **Configure**.

The dialog with the connection settings opens.

- 9) Enter under **Description** a short description for the connection.
- 10) Enter a valid e-mail address under **Default Sender Address**.

This address is used as originator address for e-mails that OpenScape UC Application sends automatically via the external SMTP server – in particular also for voice messages left via the voice portal's guest access. OpenScape UC Application sends non-delivery reports to this address also.

- 11) Enter under **SMTP Host** the IP address of the SMTP server via which OpenScape UC Application is to transmit automatically sent e-mails.

If your network has a Domain Name Service (DNS), you can also specify the host name of the associated computer system as alternative.

- 12) Specify under **Port** the port to be used by the SMTP server for the SMTP communication. This is port **25** by default.

- 13) If the SMTP server is to be enabled to communicate via TLS, activate the **Enable STARTTLS** option.

NOTICE: A STARTTLS-based connection always starts unencrypted and switches to TLS only if TLS is active for both communication partners.

- 14) If the SMTP server demands authentication, activate the option **Enable Authentication**.

In this case continue as follows:

- a) Enter under **Authentication Realm** the realm of the SMTP server.
- b) Enter under **User Name** the account name of the user to serve for accessing the SMTP server.
- c) Enter under **Password** the password for the user account you have specified in the **User Name** field.

- 15) Select **Save**.

The configuration dialog closes and the settings are saved.

Configuring the conference portal is now complete.

4.9.9 Configuring Video Systems

For operating released video systems with the conference portal, we recommend to perform the following settings at the video systems used:

- Communication via SIP
- Audio codec prioritization: G.722 over G.711

NOTICE: These settings need not be performed at every released video system.

NOTICE: All UC users participating in a video conference should be configured without silent monitoring Agent enabled in OSV, because the video streams cannot be monitored.

The following examples explain where to perform such settings.

4.9.9.1 Counterpath Bria

Codec prioritization

Softphone Preferences > Preferences > Audio Codecs > Order

SIP communication

No settings required for SIP communication.

4.9.9.2 Eyebeam

No settings required for SIP communication and codec prioritization.

4.9.9.3 Siemens VHD 100 / 400 (LifeSize Express / Team)

SIP communication

- 1) Administrator Preferences > Communications > H.323 > Disable
- 2) Administrator Preferences > Communications > SIP > Enable

Codec prioritization

Administrator Preferences > Audio > Audio Codec Order

4.9.9.4 Polycom HDX 4500

SIP communication

- 1) Administrator Settings > IP Network > SIP
- 2) Deactivate all other protocol options.

Codec prioritization

No settings for codec prioritization required.

4.9.9.5 Polycom HDX 6000

SIP communication

- 1) Administrator Settings > Network > Call Preferences > SIP
- 2) Deactivate all other protocol options.

Codec prioritization

No settings for codec prioritization required.

4.9.9.6 Polycom HDX 7000

SIP communication

- 1) Administrator Settings > IP Network > SIP
- 2) Deactivate all other protocol options.

Codec prioritization

No settings for codec prioritization required.

4.9.9.7 Polycom VVX 1500

SIP communication

- 1) H.323 > H.323 Protocol > disabled
- 2) SIP > SIP Protocol > enabled

Codec prioritization

No settings for codec prioritization required.

4.9.9.8 Tandberg E 20

No settings required for SIP communication and codec prioritization.

4.9.9.9 OpenScape Fusion

Codec prioritization

Settings > Advanced > HiPath Provider > Codec Order

SIP communication

No settings required for SIP communication.

Voice Portal

4.10 Configuring the Voice Portal

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

How to configure the voice portal:

- 1) [Configuring the User Access to the Voice Portal](#)
- 2) **If you wish to use the OpenScape UC Application voice portal as voicemail system:**
[Configuring the Guest Access to the Voice Portal](#)
- 3) **If you wish to use the voice portal or a third-party product as voicemail system:**
[Configuring a Voicemail Number for Users](#)
- 4) [Configuring the Phone Number Normalization](#)

5) If you use several Media Servers operating in parallel:

[Configuring the Voice Portal for Media Server Farm](#)

6) If you use several Media Servers operating in parallel:

[Configuring the Replication of Voice Portal Greetings](#)

These steps are described in detail in the following sections.

4.10.1 Configuring the User Access to the Voice Portal

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. Configuring such a Media Server farm is described in [Configuring the Voice Portal for Media Server Farm](#) on page 189.

The voice portal user access must be available via individual access numbers.

Start the configuration

How to configure the access numbers for the voice portal user access:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select in the list the link of the voice portal application for which you wish to configure a user access.

- Select the **Voiceportal** application, if you wish to configure a user access controlled via telephone keys.
- Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled user access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 6) Select the radio button of the application profile **start (Voice Portal access)** and select **Copy**.

The configuration dialog for a new application profile opens.

- 7) Specify under **Profile name** a name for the new application profile.

The application profile will be managed in the voice portal plug-in under this name.

- 8) Switch to the **General** tab.

- 9) Select under **Voice Portal default language** the default language for the user access to deploy.

- 10) Click on **Save** to copy the settings for the application profile.

- 11) Click on **Close** to close the configuration dialog of the voice portal plug-in.
- 12) In the OpenScope Media Server configuration dialog switch to the **Terminals** tab.
- 13) Select **Add**.

The configuration dialog for a new terminal opens.

- 14) Specify a unique identifier for the new terminal under **Terminal ID**.

Under this name the terminal is administered in the CMP.

- 15) Select the voice portal application profile you have just created under **Application**

Depending on the voice portal application used it carries a name of the following format:

- Voiceportal#<application profile name >
- Voiceportalspeech#<application profile name >

- 16) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

- 17) Specify under **Address-expression** at least one phone number under which the user access of the voice portal shall be available.

NOTICE: Calls for the defined phone numbers must be routed to the SIP trunk to the OpenScope Media Server by the communications system used. You need to configure the routing of the communications system accordingly.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScope Media Server during the connection setup.

- 18) Determine under **Type** in which format the specified address expression is to be interpreted by the OpenScope Media Server.
- 19) Click on **OK** to copy the address settings.
- 20) If required, bind further addresses to the terminal in the described manner.
- 21) Click on **Save** to copy the settings for the terminal.
- 22) If required, configure in the described manner further voice portal user accesses – e. g. user accesses with other default languages.

You have now configured the access numbers for the voice portal user access.

4.10.2 Configuring the Guest Access to the Voice Portal

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. Configuring such a Media Server farm is described in [Configuring the Voice Portal for Media Server Farm](#) on page 189.

NOTICE: You need to execute the configuration steps of this chapter only if you use the voice portal as voicemail system.

Voice messages can be left for OpenScape users via the voice portal guest access. The voice portal guest access must be available via corresponding access numbers.

Start the configuration

How to configure the access numbers for the voice portal guest access:

- 1) In the configuration dialog of the selected OpenScape Media Server switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 2) Select in the list the link of the voice portal application for which you wish to configure a guest access.
 - Select the **Voiceportal** application, if you wish to configure a telephone-controlled guest access.
 - Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled guest access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 3) Select the radio button of the application profile **guest (Guest Portal access)** and select **Copy**.

The configuration dialog for a new application profile opens.

- 4) Specify under **Profile name** a name for the new application profile.

The application profile will be managed in the voice portal plug-in under this name.

- 5) Switch to the **General** tab.
- 6) Select under **Voice Portal default language** the default language for the guest access to deploy.
- 7) Click on **Save** to copy the settings for the application profile.
- 8) Click on **Close** to close the configuration dialog of the voice portal plug-in.
- 9) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
- 10) Select **Add**.

The configuration dialog for a new terminal opens.

- 11) Specify a unique identifier for the new terminal under **Terminal ID**.

Under this name the terminal is administered in the CMP.

- 12) Select the voice portal application profile you have just created under **Application**.

Depending on the voice portal application used it carries a name of the following format:

- Voiceportal#<application profile name >
- Voiceportalspeech#<application profile name >

- 13) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

- 14) Specify under **Address-expression** at least one phone number under which the guest access shall be available.

NOTICE: Calls for the defined phone numbers must be routed to the SIP trunk to the OpenScape Media Server by the communications system used. You need to configure the routing of the communications system accordingly.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

- 15) Determine under **Type** in which format the specified address expression is to be interpreted by the OpenScape Media Server.
- 16) Click on **OK** to copy the address settings.
- 17) If required, bind further addresses to the terminal in the described manner.
- 18) Click on **Save** to copy the settings for the terminal.
- 19) If required, configure in the described manner further voice portal guest accesses – e. g. guest accesses with other default languages.

You have now configured the access numbers for the voice portal guest access.

4.10.3 Configuring a Voicemail Number for Users

NOTICE: You need to execute the configuration steps of this chapter only if you do not use OpenScape Xpressions as voicemail system.

OpenScape UC Application uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called user. In this way no call is lost even if the called user cannot answer the phone.

The number under which a user's voicemail box can be reached depends on the voicemail system you use with the OpenScape system.

- Using OpenScape Xpressions or a third-party product as voicemail system In this case a caller is routed to the PhoneMail script of the OpenScape Xpressions server or to the voicemail system of a third-party supplier, if the callee cannot accept the call.
- Using the voice portal as voicemail system In this case a caller is routed to the guest access of the voice portal if the callee cannot accept the call.

You can assign the number of your voicemail box to users either manually or by bulk import. How to use bulk import is described in the *OpenScape Common Management Platform, Administrator Documentation* manual.

NOTICE: If you do not assign a voicemail number to a user, calls will not be automatically forwarded to the user's voicebox.

Start the configuration

How to assign a user a voicemail number manually:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain in which the relevant user account has been created.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **Accounts > List**.

A list of all users configured in the selected domain appears in the workspace.

- 4) Click on the login name of the desired user.

The dialog with the settings of the relevant user opens.

- 5) Switch to the **Resources** tab.

All resources assigned to the user are displayed.

- 6) Click on **Assign**.

A list of all phone numbers that can be assigned as voicemail number to the user appears.

If the list does not contain any phone numbers, you need to create a new phone number. Proceed as follows:

- a) Click the **Add** button.

The dialog for creating a new voicemail number opens.

- b) Enter in the **Number** field the voicemail number to which incoming calls may be routed for the relevant user. If you use the voice portal as voicemail system, this number is the access number for the guest access you configured in [Configuring the Guest Access to the Voice Portal](#) on page 184.

- c) Click **OK** to create the new phone number.

The newly created phone number is now displayed in the phone number list.

- 7) Select the radio button of the voicemail number to which incoming calls are to be routed for the relevant user in due course. If you use the voice portal as voicemail system, this number is the access number for the guest access you configured in [Configuring the Guest Access to the Voice Portal](#) on page 184.
- 8) Click on **OK** to copy the selected phone number for the user.
- 9) Click on **Save** to copy the settings.

You have now manually assigned a voicemail number to the user.

4.10.4 Configuring the Phone Number Normalization

NOTICE: If you use several Media Servers operating in parallel, skip this chapter. Configuring such a Media Server farm is described in [Configuring the Voice Portal for Media Server Farm](#) on page 189.

If e.g. a user needs to specify a phone number in the voice portal, he/she will do this always with reference to the respective location. For example, as pure extension or as phone number with area code but without international prefix. But this leads to problems if the voice portal e.g. is located in a country different from the user's.

To evade such phone number problems, the OpenScape system transforms all phone numbers before the actual processing into a normalized phone number format – e. g. +492404901100. The thus normalized phone numbers then contain all information that the phone number uniquely identifies or localizes.

The OpenScape system may use so-called address translation contexts for this phone number normalization.

If an OpenScape user enters a phone number via the voice portal TUI, the voice portal uses the information of the relevant OpenScape user as address translation context. If this is not possible, the voice portal uses address translation contexts that can be configured in the CMP instead.

You can assign an individual address translation context to each application profile of the voice portal.

Start the configuration

How to configure the address translation context for a voice portal access:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select in the list the link of the voice portal application for which you have configured user or guest accesses.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 6) Select the name of the application profile for which you wish to configure the address translation context.

The configuration dialog for the application profile opens.

- 7) Switch to the **General** tab.

- 8) Select under **Address translation context** the context you wish to use for the relevant application profile.

NOTICE: This address translation context must have previously been configured in the CMP. Compare [Configuring Address Translation Contexts](#) on page 140.

- 9) Click on **Save** to copy the settings for the application profile.

- 10) Click on **Close** to close the configuration dialog of the voice portal plug-in.

- 11) Configure the phone number context in the described manner for all created application profiles.

You have now configured the phone number normalization for the user or guest accesses of the voice portal.

4.10.5 Configuring the Voice Portal for Media Server Farm

NOTICE: You need to execute the configuration steps of this chapter only if you use several Media Server servers operating in parallel.

NOTICE: You find a description of how the voice portal uses the configuration outlined in the following in the *OpenScape Media Server, Administrator Documentation* manual.

NOTICE: The numbering scheme used in this chapter is merely an example to illustrate the correlations in the system configuration. You can also choose an approach similar to this numbering scheme but better suited for the available system environment.

You can use OpenScape UC Application with several OpenScape Media Servers operating in parallel – a so-called Media Server farm.

Start the configuration

Configure the conference portals of the different OpenScape Media Servers for a Media Server farm by following the steps of the following guide.

- 1) Configure in OpenScape Voice a new endpoint in the global numbering plan for each OpenScape Media Server of the Media Server farm.
 - a) On the **General** tab activate for each endpoint the **Registered** option.
 - b) Select on the **SIP** tab type **Static** for each endpoint.
 - c) Specify the IP address of the respective OpenScape Media Server in the **Endpoint Address** field.
 - d) Switch to the **Attributes** tab and activate the **Allow Sending of Insecure Referred-By Headers** option. Switch to the **Attributes** tab and activate the **Send International Numbers in Global Number Format (GNF)** option. OpenScape Voice then sends all GNF-based phone numbers with a leading + character to the OpenScape Media Server.

Example of a Media Server farm with two OpenScape Media Servers:

	Endpoint 1	Endpoint 2
Endpoint name:	EP_MS-1	EP_MS-2
Endpoint IP address:	10.1.1.21	10.1.1.22

NOTICE: You can use these endpoints for the voice as well as for the conference portal of a Media Server farm.

- 2) Configure a new shared destination in the global numbering plan in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

Example: DEST_MS-ALL

- 3) Create in the shared destination a route to each of the OpenScape Media Servers.

- a) Assign an individual ID to each route.
- b) In doing so, select the **SIP Endpoint** option for **Endpoint Type**.
- c) Select under **SIP Endpoint** the endpoint of the respective OpenScape Media Server.
- d) Select under **Modification Type** the **Number Manipulation** option.
- e) Select under **Nature of Address** the **International** option.

Example of a Media Server farm with two OpenScape Media Servers:

Destination:	Routes	
DEST_MS-ALL	Route 1	Route 2
ID:	1	2
SIP Endpoint:	EP_MS-1	EP_MS-2

NOTICE: You can use this shared destination for the voice as well as for the conference portal of a Media Server farm.

- 4) Configure a shared prefix access code in the global numbering plan in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

Callers will be able to reach the voice portal of all OpenScape Media Servers under this prefix access code.

Use the following format for the prefix access code:

<GNF Prefix Replacement><Country Code><Area Code>
><Local Office Code><Extension "minus one digit">

Example: 0004924040901120

The following applies:

<GNF Prefix Replacement>	:	000
<Country Code>	:	49
<Area Code>	:	240
<Local Office Code>	:	40901

<Extension >	:	1200

For this example, enter digit 3 under **Digit Position** to cut the leading digit sequence **000**. This will ensure that the phone number matches the destination code to be configured at a later date.

NOTICE: You can use this shared prefix access code for the voice as well as for the conference portal of a Media Server farm.

- 5) Configure a shared destination code in OpenScape Voice for all OpenScape Media Servers of the Media Server farm.

The voice portal of all OpenScape Media Servers will be accessible under this destination code.

In doing so, select the shared destination of all OpenScape Media Servers under **Destination Name**.

Use for example the following format for the destination code:

<Country Code><Area Code><Local Office Code><Extension “minus one digit”>

Example: 4924040901120

NOTICE: You can use this shared destination code for the voice as well as for the conference portal of a Media Server farm.

- 6) If the endpoints of the OpenScape Media Servers and the OpenScape Voice subscribers are configured under different numbering plans, you must configure comparable destinations, routes, prefix access codes and destination codes for all involved numbering plans.

This applies e. g. if the OpenScape Voice subscribers are configured under a private numbering plan and the OpenScape Media Server endpoints under E.164.

- 7) Configure the same phone number for the user access and the same phone number for the guest access on each OpenScape Media Server of the Media Server farm.

Proceed as described in the following sections and consider the destination code you have configured in step 5.

- [Configuring the User Access to the Voice Portal](#) on page 183
- [Configuring the Guest Access to the Voice Portal](#) on page 184

Example of a Media Server farm with two OpenScape Media Servers and the example destination code from step 5:

	Media Server 1	Media Server 2
Phone number user access	49240409011205	49240409011205
Phone number guest access	49240409011206	49240409011206

- 8) If required, configure the multilingual voice portal accesses in the same way.

- 9) Configure the phone number normalization of the voice portal for each OpenScape Media Server of the Media Server farm. Proceed as described in [Configuring the Phone Number Normalization](#) on page 187.

After this configuration the conference portal solution is now operable for a Media Server farm.

4.10.6 Configuring the Replication of Voice Portal Greetings

NOTICE: You need to execute the configuration steps of this chapter only if you use several Media Server servers operating in parallel.

If the OpenScape Media Server is used in a Media Server farm, it can automatically replicate customized voice portal welcome and name greetings to all other OpenScape Media Servers of the farm.

Start the configuration

How to configure the automatic replication of the modified voice portal announcements:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) Click the name of the OpenScape Media Server for which you want to configure the replication.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the OpenScape Media Server configuration dialog switch to the **Providers** tab.

- 5) Select the **Replicate Node** link in the provider list.

The configuration dialog with the settings of the prompt replication group opens.

- 6) Select **Add Node....**

This opens the configuration dialog in which all remote OpenScape Media Servers of the Media Server farm are displayed.

- 7) Tick the check boxes of all displayed OpenScape Media Server servers.

- 8) Select **OK**.

The settings of the prompt replication group now display the selected OpenScape Media Servers as part of the replication group.

- 9) Select **Save** to copy the new settings of the prompt replication group.

- 10) Execute the described steps on every OpenScape Media Server of the Media Server farm.

Customized voice portal greetings are then automatically replicated on all OpenScape Media Servers of the Media server farm.

Configuring the voice portal is now complete.

4.11 Connecting Microsoft Exchange

You can connect OpenScape UC Application to different Microsoft Exchange versions. How to proceed depends on the Microsoft Exchange version used.

The following sections describe the configuration steps that you need to execute for connecting the respective Microsoft Exchange system.

- [Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019](#)

4.11.1 Configuring the Connection to Microsoft Exchange 2013/ 2016 / 2019

NOTICE: Special requirements must have been met for configuring the Microsoft Exchange connection. See [Configuration requirements for the Microsoft Exchange connection](#) on page 83.

If you configure the Microsoft Exchange connection for Microsoft Exchange 2013 or Microsoft Exchange 2016 or Microsoft Exchange 2019, you cannot connect any of the following systems to the OpenScape system additionally:

- Other Microsoft Exchange versions
- IBM Lotus Domino

How to configure the Microsoft Exchange connection for Microsoft Exchange 2013 / 2016 / 2019:

- 1) [Configuring a technical User Account for Microsoft Exchange 2013 / 2016 / 2019](#) on page 194
- 2) [Configuring the Receive Connector for Microsoft Exchange 2013/ 2016 / 2019](#) on page 195
- 3) [Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019](#) on page 198
- 4) [Configuring the Groupware-Exchange Connector for Microsoft Exchange 2013 / 2016 / 2019](#) on page 199
- 5) [Creating User Assignments for Microsoft Exchange 2013/ 2016 / 2019](#) on page 204
- 6) [Importing User Assignments for Microsoft Exchange 2013/ 2016 / 2019](#) on page 209
- 7) [Configuring Access to Microsoft Outlook Contacts for Microsoft Exchange 2013/ 2016 / 2019](#) on page 210
- 8) [Configuring restricted Access to private Microsoft Exchange 2013/ 2016 / 2019 Contacts](#) on page 211

These steps are described in detail in the following sections.

You find continuative information about the technical design of the Microsoft Exchange connection in [Microsoft Exchange Connection](#) on page 32.

4.11.1.1 Configuring a technical User Account for Microsoft Exchange 2013 / 2016 / 2019

The Groupware-Exchange connector uses a technical user account for accessing the Web Services interface of Microsoft Exchange. You will have created this user account already in the corresponding Active Directory domain to comply with the configuration requirements.

This technical user account must be allowed using impersonation.

NOTICE: The following description allows impersonation restricted to the users of a single organization unit. Alternatively, you can assign impersonation in a different way – e. g. restricted to the users of an entire organization. You find impersonation details in the Microsoft Exchange 2013 / 2016 / 2019 product information.

Start the configuration

How to allow impersonation for the technical user account restricted to the users of a single organization unit:

- 1) Open the Microsoft Exchange management shell.
- 2) Execute the following command in one line to create a new management scope on the users of the relevant organization unit – for example a scope with the name OSUCscope on the users of the organization unit with the fully qualified name unify.com/sales/salesEMEA.

```
New-ManagementScope -Name "OSUCscope"  
-RecipientRoot "unify.com/sales/salesEMEA"  
-RecipientRestrictionFilter {RecipientType  
-eq "UserMailbox"}
```

- 3) Execute the following command to check whether the previous command was executed correctly.

```
Get-ManagementScope "OSUCscope" | Format-List
```

- 4) Execute the following command in one line to allow the technical user account impersonation via a new management role assignment and the new management scope – e. g. via a management role assignment named impersonationOSA .

```
New-ManagementRoleAssignment  
-Name:impersonationOSA  
-Role:ApplicationImpersonation  
-User:<techn. user account>  
-CustomRecipientWriteScope:OSUCscope
```

- 5) Execute the following command in one line to check whether the previous command was executed correctly.

```
Get-ManagementRoleAssignment  
-CustomRecipientWriteScope OSUCscope | Format-List
```

Output example, in which the techn. user account OSUC belongs to the organization unit with the fully qualified name unify.com/ServiceAccounts:

```

RunspaceId : e245765e-b469-4010-9a88-b2c4ae82eb32
User : unify.com/ServiceAccounts/OSUC
AssignmentMethod : Direct
Identity : impersonationOSA
EffectiveUserName : OSUC
AssignmentChain :
RoleAssigneeType : User
RoleAssignee : unify.com/ServiceAccounts/OSUC
Role : ApplicationImpersonation
CustomRecipientWriteScope : OSUCscope
CustomConfigWriteScope :
RecipientReadScope : Organization
ConfigReadScope : None
RecipientWriteScope : CustomRecipientScope
ConfigWriteScope : None
Enabled : True
RoleAssigneeName : OSUC
IsValid : True
ExchangeVersion : 0.11 (14.0.550.0)
Name : impersonationOSA

DistinguishedName : CN=impersonationOSA,CN=Role
Assignments,CN=RBAC,
CN=XCHORG,CN=Microsoft
Exchange,CN=Services,CN=Configuration,
DC=unify,DC=com

Guid : 605bdc30-c98f-4874-b89b-fa7506176ab2
ObjectCategory : unify.com/Configuration/Schema/ms-Exch-
Role-Assignment
ObjectClass : {top, msExchRoleAssignment}
WhenChanged : 9/1/2020 2:53:36 PM
WhenCreated : 9/1/2020 2:53:36 PM
WhenChangedUTC : 9/1/2020 12:53:36 PM
WhenCreatedUTC : 9/1/2020 12:53:36 PM
OrganizationId :
OriginatingServer : DC1.unify.com

```

You have now prepared the technical user account for connecting OpenScape UC Application.

4.11.1.2 Configuring the Receive Connector for Microsoft Exchange 2013/ 2016 / 2019

OpenScape UC Application uses the SMTP server of the Microsoft Exchange system for sending independently created e-mails to the e-mail inboxes of the Microsoft Exchange system. To enable this, a new receive connector must be configured in the Microsoft Exchange system. This connector is exclusively used for connecting OpenScape UC Application and Microsoft Exchange.

There are two basic options for configuring this receive connector.

- As receive connector with authentication

[Example of configuring a Receive Connector with Authentication](#)

- As receive connector without authentication (anonymous relaying)

Example of configuring a Receive Connector without Authentication

How to create a receive connector for Microsoft Exchange is described in the producer's instructions under the following link:

<http://technet.microsoft.com/en-us/library/bb125128.aspx>

A guide to creating a receive connector without authentication is available under the following link:

<http://exchangeopedia.com/2007/01/exchange-server-2007-how-to-allow-relaying.html>

IMPORTANT: Execute this step with care. An incorrect configuration may enable unauthorized persons to send e-mails via the Microsoft Exchange system.

NOTICE: Verify that the connection settings of the Groupware-Exchange connector correspond to the privileges of the receive connector used.

Example of configuring a Receive Connector with Authentication

- 1) Execute the following command in the Microsoft Exchange Management Shell in one line to configure a new receive connector with authentication for sending e-mails:

```
New-ReceiveConnector
-Name "< connector name >"
-Usage Custom-AuthMechanism Tls, BasicAuth,
  BasiAuthRequireTLS
-PermissionGroups ExchangeUsers
-Bindings < IP address >:< port >
-RemoteIpRanges < IP address of the application
  computer >
```

*Example:*⁷ The following example command creates a receive connector called OSUC-Relay, which uses the local address 10.2.3.4:25 for reacting to transmissions from the address 192.168.5.77.

```
New-ReceiveConnector
-Name "OSUC-Relay"
-Usage Custom
-AuthMechanism Tls, BasicAuth, BasiAuthRequireTLS
-PermissionGroups ExchangeUsers
-Bindings 10.2.3.4:25 -RemoteIpRanges 192.168.5.77
```

- 2) Execute the following command in the Microsoft Exchange Management Shell in one line for allowing the deployed technical user account to send e-mails:

```
Get-ReceiveConnector "OSUC-Relay" | Add-ADPermission
```

⁷ The product documentation for Microsoft Exchange describes configuration details of this command and alternative configuration methods.


```
-User "unify\OSUC"
-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

Example:⁷ The following example command entitles the user account OSUC of the domain unify.com to send e-mails.

```
Get-ReceiveConnector "OSUC-Relay" | Add-ADPermission -
User "unify\OSUC"
-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

- 3) To enable the deployed technical user account sending e-mails on behalf of other Microsoft Exchange users, it requires the following advanced Microsoft Exchange privileges for all Microsoft Exchange users that deploy the OpenScape UC Application.
 - Send-As
 - Ms-Exch-SMTP-Accept-Any-Sender
- 4) Verify that the connection settings of the Groupware-Exchange connector correspond to the privileges configured for the receive connector used.

NOTICE: Please note the following for voice messages left by callers e.g. in the voice portal's guest access and sent to the relevant OpenScape users as e-mail: If the Microsoft Exchange server can resolve the deployed technical user account in a display name, the inbox displays for the associated e-mail the mailbox name of the technical user account as originator address and not the originator number of the caller.

Example of configuring a Receive Connector without Authentication

- 1) Execute the following command in the Microsoft Exchange Management Shell in one line to configure a new receive connector without authentication for sending e-mails:

```
New-ReceiveConnector
-Name "<connector name>"
-Usage Custom
-PermissionGroups AnonymousUsers
-Bindings <IP address>:<Port>
-RemoteIpRanges <IP address of the application computer>
```

Example:⁸ The following example command creates a receive connector called OSUC-Relay, which uses the local address 10.2.3.4:25 for reacting to transmissions from the address 192.168.5.77.

```
New-ReceiveConnector
-Name "Anonymous OSUC-Relay"
-Usage Custom
-PermissionGroups AnonymousUsers
-Bindings 10.2.3.4:25
-RemoteIpRanges 192.168.5.77
```

⁸ The product documentation for Microsoft Exchange describes configuration details of this command and alternative configuration methods.

- 2) Execute the following command in the Microsoft Exchange Management Shell in one line for allowing the deployed technical user account to send e-mails anonymously:

```
Get-ReceiveConnector "<connector name>" | Add-ADPermission
-User "<domain>\<technical user account>"
-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

*Example:*⁸ The following example command entitles the user account OSUC of the domain unify.com to send e-mails anonymously.

```
Get-ReceiveConnector "Anonymous OSUC-Relay" | Add-ADPermission
-User "unify\OSUC"
-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

- 3) Verify that the connection settings of the Groupware-Exchange connector correspond to the privileges configured for the receive connector used.

NOTICE: Please note the following for voice messages left by callers e.g. in the voice portal's guest access and sent to the relevant OpenScape users as e-mail: If the Microsoft Exchange server can resolve the deployed technical user account in a display name, the inbox displays for the associated e-mail the mailbox name of the technical user account as originator address and not the originator number of the caller.

4.11.1.3 Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019

OpenScape UC Application uses the Autodiscover service for dynamically determining the Web Services URL via which the mailboxes of individual OpenScape users can be accessed.

If the Autodiscover service is activated for a web-services-based Microsoft Exchange connection, the Groupware-Exchange connector sends the e-mail address of the relevant OpenScape user as Autodiscover request to the URL of the Autodiscover service. Thereupon, the Autodiscover service returns the current Web Services URL of the CAS via which the mailbox of the relevant user can be accessed. Subsequently, the Groupware-Exchange connector can connect to this Web Services URL and access the user mailbox of the respective OpenScape user.

The Autodiscover service can return two different Web Services URLs upon request:

- One internal Web Services URL This URL is required by the Groupware-Exchange connector if the relevant Web Services can be reached within a corporate network without firewall transitions.
- One external Web Services URL This URL is required by the Groupware-Exchange connector if the relevant Web Services can only be reached via firewall barriers.

IMPORTANT: To transmit external Web Services URLs to the Groupware-Exchange connector via Autodiscover, the Outlook Anywhere function must be active on every CAS that publishes Web Services URLs via Autodiscover.

You find further information about the work mode of the Autodiscover service under the following link:

<http://technet.microsoft.com/en-us/library/bb124251.aspx>

Start the configuration

How to configure the internal and external Web Services URL for a CAS:

- 1) Open the Microsoft Exchange management shell on the CAS.
- 2) If the Autodiscover service is to publish an external Web Services URL for the relevant CAS, execute the following command in one line to define this URL:

```
Set-WebServicesVirtualDirectory -identity "<virtual directory of the Web Services9>" -externalurl <external address for the Web Services of the CAS> -BasicAuthentication:$True
```

*Example:*¹⁰ The following example command defines the external address <https://mail.comp.com/EWS/> for the Web Services of the virtual directory CAS01\EWS, with CAS01 being the name of the CAS.

```
Set-WebServicesVirtualDirectory
-identity "CAS01\EWS"
-externalurl https://mail.comp.com/EWS/Exchange.asmx -
BasicAuthentication:$True
```

- 3) If the Autodiscover service is to publish an internal Web Services URL for the relevant CAS, execute the following command in one line to define this URL:

```
Set-WebServicesVirtualDirectory
-identity "<virtual directory of the Web Services>"
-internalurl <internal address for the Web Services of the CAS>
-BasicAuthentication:$True
```

Depending on the requirement, you have now configured the internal or external Web Services URL for the CAS.

4.11.1.4 Configuring the Groupware-Exchange Connector for Microsoft Exchange 2013 / 2016 / 2019

In [Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019](#) on page 198 we described the basic work mode of the Autodiscover service. You can operate this service in two modes.

⁹ You can determine this directory by the following command: `Get-WebServicesVirtualDirectory`

¹⁰ The product documentation for Microsoft Exchange describes configuration details of this command and alternative configuration methods.

- **Dynamic Autodiscover** In this mode, the Groupware-Exchange connector creates the required Autodiscover URL dynamically from the SMTP domain of the addressed e-mail address.

Example of deriving the URL in case of the static Autodiscover: The e-mail address `user@comp.com` of user *user* is assigned to the SMTP domain `comp.com`. In this case the Groupware-Exchange connector sends Autodiscover requests to the following derived Autodiscover URL:

`https://comp.com/autodiscover/autodiscover.xml`

You can prefix the thus dynamically created Autodiscover URLs as follows – e. g. in the event that the CAS have host names of the format `<prefix>.comp.com`.

`https://<prefix>.comp.com/autodiscover/autodiscover.xml`

NOTICE: Dynamic Autodiscover uses exclusively encrypted communication (HTTPS).

- **Static Autodiscover** In this mode the Groupware-Exchange provider sends Autodiscover requests always to the same statically configured Autodiscover URL.

NOTICE: The host part of all Autodiscover URLs must be resolvable via DNS. This concerns the statically as well as dynamically created Autodiscover URLs. Furthermore, all Autodiscover URLs must always refer to CAS that can publish Web Services URLs upon Autodiscover requests.

The Groupware-Exchange connector uses a technical user account for accessing the Web Services interface of Microsoft Exchange. You will have created this user account already in the corresponding Active Directory domain to comply with the configuration requirements.

Start the configuration

How to configure the Groupware-Exchange connector:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select **Add**.

The dialog for adding a new groupware connection opens.

- 5) Select under **Connection Type** the entry **Microsoft Exchange Web Services**.
- 6) Specify a unique identifier for the connection under **Connection ID**.

Example: ConnectionMSE2019

You will later use this identifier to assign this connection to OpenScape users.

- 7) Select **Save**.

The new connection is displayed in the list of all configured groupware connections.

- 8) Select the radio button of the connection you have just added.
9) Select **Configure**.

The configuration dialog of the selected connection opens.

- 10) Verify that the **Exchange Web Services Configuration** tab is displayed.
11) Specify under **Domain** the name of the Windows domain that hosts the Microsoft Exchange server.

In doing so use the NetBIOS name.

Example:

Domain name fully qualified:	EXCH.unify.com
Domain name NetBIOS:	EXCH

- 12) Enter the name of the technical user account in the **Technical User Account** field.
13) Enter the password of the technical user account in the **Password** field.

NOTICE: The Groupware-Exchange connector attempts to log on to the Microsoft Exchange server with the following authentication processes in the given sequence: – BASIC – DIGEST – NTLM

NOTICE: Using NTLM v2 requires performing the following in the EWS settings of Microsoft Exchange: – Authentication processes BASIC and DIGEST disabled – Windows authentication active (default setting) – Anonymous authentication as is default in the EWS settings
You find information about the Microsoft Exchange default settings depending on the version for example under the following links: Microsoft Exchange Server 2013: <https://docs.microsoft.com/en-us/exchange/default-settings-for-exchange-virtual-directories-exchange-2013-help> Microsoft Exchange Server 2016/2019: <https://docs.microsoft.com/en-us/exchange/clients/default-virtual-directory-settings?view=exchserver-2019>

- 14) Select one of the following options under **Exchange Access Mode**:
- **Static Autodiscovery** for activating the static mode of Autodiscover.
 - **Dynamic Autodiscovery** for activating the dynamic mode of Autodiscover.
- 15) If you have selected the **Static Autodiscovery** option under **Exchange Access Mode**:

Specify under **Autodiscover URL** the static address for the Groupware-Exchange connector to send Autodiscover requests to.

Example: `https://exchange.domain154/autodiscover/autodiscover.xml`

- 16) If you have selected the **Dynamic Autodiscovery** option under **Exchange Access Mode**:

If required, enter a prefix under **Autodiscover URL Prefix** to be considered when deriving the Autodiscover URL dynamically.

- 17) Select one of the following options under **Autodiscover Protocol**:

- **Internal** if OpenScape UC Application can reach the URLs of all Web Services within a corporate network without firewall transitions.
- **External** if OpenScape UC Application can reach the Web Services URLs via firewall barriers only.

- 18) When you have performed all Groupware-Exchange connector settings by the end of this chapter you can check whether the Microsoft Exchange connection works correctly. Specify for this test a primary e-mail address under **Primary Email address of the Test Mailbox**. This primary address must be available as valid address in one of the connected Microsoft Exchange servers.

NOTICE: The specified address is only used to test the Microsoft Exchange connection functionality.

- 19) Switch to the **SMTP Configuration** tab.

- 20) Enter in the **Default Sender Address** field an e-mail address available in the Microsoft Exchange server as valid address.

This address is used as originator address for e-mails that OpenScape UC Application automatically sends via the SMTP server of the Microsoft Exchange server – thus e. g. for voice messages left via the voice portal's guest access. OpenScape UC Application sends non-delivery reports to this address also.

NOTICE: Please note the following for voice messages left by callers e.g. in the voice portal's guest access and sent to the relevant OpenScape users as e-mail: If the Microsoft Exchange server can resolve the deployed technical user account in a display name, the inbox displays for the associated e-mail the mailbox name of the technical user account as originator address and not the originator number of the caller.

NOTICE: In case of a Microsoft Exchange 2013 / 2016 / 2019 connection based on Web Services please note the following: If the voice portal is used for playing voicemail messages sent by the OpenScape UC Application via the MS Exchange server, the display name of the user account associated to the e-mail address under Default Sender Address is always announced as originator of the message."

- 21) In the **SMTP Host** field enter the IP address under which the SMTP server of the Microsoft Exchange server can be reached.

If your network has a Domain Name Service (DNS), you can also specify the host name of the associated computer system as alternative.

- 22) Specify in the **Port number** field the port to be used by the Groupware-Exchange connector for the SMTP communication. This is port **25** by default.
- 23) If the SMTP server is to enabled to communicate via TLS, activate the **Enable STARTTLS** option.

This requires TLS to be active on the SMTP server also.

NOTICE: A STARTTLS-based connection always starts unencrypted and switches to TLS only if TLS is active for both communication partners.

- 24) If the SMTP server demands authentication, activate the option **Enable Authentication**.

In this case continue as follows:

NOTICE: You need to perform authentication settings only if you have configured a receive connector with authentication in [Configuring the Receive Connector for Microsoft Exchange 2013/ 2016 / 2019](#) on page 195. If you have configured anonymous e-mail sending for the receive connector used, no authentication settings are required.

- a) Enter under **User Name** the account name of the user to serve for accessing the SMTP server.
- b) Enter under **Password** the password for the user account you have specified in the **User Name** field.

NOTICE: The Groupware-Exchange connector attempts to log on to the Microsoft Exchange server with the following authentication processes in the given sequence:

- BASIC
 - DIGEST
 - NTLM
-

NOTICE: Using NTLM v2 requires performing the following in the EWS settings of Microsoft Exchange: –

- Authentication processes BASIC and DIGEST disabled
- Windows authentication active (default setting)

- Anonymous authentication as is default in the EWS settings

You find information about the Microsoft Exchange default settings depending on the version for example under the following links: Microsoft Exchange 2013:

[http://technet.microsoft.com/en-us/library/gg247612\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/gg247612(v=exchg.150).aspx)

Microsoft Exchange 2016/2019:

[https://technet.microsoft.com/en-us/library/mt634322\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/mt634322(v=exchg.160).aspx)

25) Select **Save.**

The configuration dialog closes and the settings are saved.

26) Select the radio button of the just configured Groupware-Exchange connector and click on **Test.**

If the test fails, the Groupware-Exchange connector cannot connect to the Microsoft Exchange organization trouble-free. Check in this case all Groupware-Exchange connector settings and the settings on the Microsoft Exchange side once more.

27) If you have configured dynamic Autodiscover or a HTTPS URL on the **Exchange Web Services Configuration, information is automatically transmitted securely between the Groupware-Exchange connector and the systems of the Microsoft Exchange organization. To this, the public keys of all required SSL certificates must be made known to the Groupware-Exchange connector.**

How to proceed is described in [Configuring the encrypted Transmission between Groupware-Exchange Connector and Microsoft Exchange Servers](#) on page 435.

You have thus completely configured the Groupware-Exchange connector.

4.11.1.5 Creating User Assignments for Microsoft Exchange 2013/ 2016 / 2019

To ensure a smoothly operating Microsoft Exchange connection, you need to assign the respectively associated Microsoft Exchange user accounts to the relevant OpenScape user accounts. Import the corresponding user assignments in OpenScape UC Application for this purpose.

NOTICE: If the OpenScape user data was copied from the Microsoft Exchange system automatically, user assignments can be configured automatically as far as possible. The Unified Communication templates in the CMP's user management are used for this purpose. How to use the templates in the CMP's user management is outlined in the *OpenScape Common Management Platform, Administrator Documentation* manual. In contrast, you can use the descriptions in the chapters that follow also if the OpenScape user data was not copied from the Microsoft Exchange System automatically.

Before you can import the user assignments in OpenScape UC Application you need to create the relevant assignments.

Start the configuration

How to create the user assignments:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.

The dialog for exporting configurations opens.

- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.
- 8) Open the downloaded Zip file and open the following Zip file contained therein:

```
{exportWorkingDir}\
Package_domainmanagement_domainmanagement001.zip
```

- 9) In there open the following file with a text editor:

```
{BackupApplWorkDir}\domain_configuration.csv
```

NOTICE: If the data is to contain special characters, you need to use a text editor that supports the UTF-8 file format. Microsoft Windows Wordpad and Microsoft Word do not support the UTF-8 file format. Notepad does.

NOTICE: The text editor used must not deploy a Byte-Order-Mark – BOM.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the user assignments under the entry that begins with **##ExternalId**.
- The fields of an entry are separated from each other by semicolon.

- 10) Add all required user assignments to the exported `domain_configuration.csv` file under `##ExternalId`.

In doing so please heed the following:

- The following data special characters must be marked by the escape character `\` for later import: `, \ # =`
- Create for each assignment of OpenScape user account and Microsoft Exchange user account a new `ExternalId` entry.
- Enter the reserved name **ExternalId** under **##ExternalId**.

This name defines the entry as user assignment.

- Specify under **externalId** a name that is unique for all `ExternalId` entries in the OpenScape system.

For example, use the e-mail address of the associated user or number the entries consecutively.

- Always specify the **false** value under **isContactMaster**.
- Always specify the **false** value under **isProvisioningMaster**.
- Specify under **assignedExternalSystemId** the unique name you have determined in the **Connection ID** field of the Groupware-Exchange connector (cf. [Configuring the Groupware-Exchange Connector for Microsoft Exchange 2013 / 2016 / 2019](#) on page 199).
- Specify under **additionalInfo** the following information and separate it with a comma:

a) Groupware_Mailbox:	<Short name of the MS Exchange user>
a) Groupware_Address:	<E-mail address of the MS Exchange user>
a) GwType:	Exchange

- Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: `mSample@system`

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	isContactMaster	isProvisioningMaster	...
ExternalId	1	false	false	...
ExternalId	2	false	false	...
...	...	...	...	...

additionalInfo	...
Groupware_Mailbox:mSample,Groupware_Address:mSample@co.com,GwType:exchange	...
Groupware_Mailbox:tBrown,Groupware_Address:tBrown@co.com,GwType:exchange	...

additionalInfo	...
...	...

assignedExternalSystemId	assignedUserIdentity
ConnectionMSE2007	mSample@system
ConnectionMSE2007	tBrown@system
...	...

```
##ExternalId;externalId;isContactMaster;
isProvisioningMaster;additionalInfo;
assignedExternalSystemId;assignedUserIdentity
```

```
ExternalId;1;false;false;Groupware_Mailbox:mSample,
Groupware_Address:mSample@co.com.com,GwType:exchange;
ConnectionMSE2007;mSample@system
```

```
ExternalId;2;false;false;Groupware_Mailbox:tBrown,
Groupware_Address:tBrown@co.com.com,GwType:exchange;
ConnectionMSE2007;tBrown@system
```

- 11)** In the exported file `domain_configuration.csv` under `##ExternalId` add all required user assignments that assign the respectively associated

Microsoft Exchange e-mail account to the relevant OpenScape user accounts. This assignment is required for the voice portal.

Please note: Create for each assignment of OpenScape user account and Microsoft Exchange e-mail account a new ExternalId entry.

How to specify the data for a new user assignment:

- a) Enter the reserved name **ExternalId** in the user entry under **##ExternalId**.

This name defines the entry as user assignment.

NOTICE: The ExternalID can be also modified in corresponding ExternalID tab in CMP

- b) Specify under **externalId** the unique Microsoft Exchange e-mail account of the relevant OpenScape user.
- c) Always specify the **false** value under **isContactMaster**.
- d) Always specify the **false** value under **isProvisioningMaster**.
- e) Always specify the **Groupware_Domain** value under **assignedExternalSystemId**. Do not specify a value under **additionalInfo**.
- f) Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: mSample@system

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	isContactMaster	isProvisioningMaster	...
ExternalId	mSample@co.com	false	false	...
ExternalId	tBrown@co.com	false	false	...
...	...	...	...	...

additionalInfo	...	assignedExternalSystemId	assignedUserIdentity
	...	Groupware_Domain	mSample@system
	...	Groupware_Domain	tBrown@system
...	...	...	...

```
##ExternalId;externalId;
isContactMaster;
isProvisioningMaster;
additionalInfo;assignedExternalSystemId;
assignedUserIdentity
```

```

ExternalId;mSample@co.com;
false;false;;
Groupware_Domain;mSample@system

ExternalId;tBrown@co.com;false;false;;
Groupware_Domain;tBrown@system
...

```

- 12) Save the supplemented file `domain_configuration.csv` in the CSV format.
- 13) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

You have now created the required user assignments.

Start the configuration

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.

The dialog for importing a configuration opens

- 4) In the **Import** file field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file
- 5) Click on **Next**.
- 6) Check that the **Common Management Platform** option has been selected under **Type of file to be imported**.
- 7) Check that the **Domain Management** option has been selected under **Included type of data**.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

You have now imported the user assignments in OpenScape UC Application.

4.11.1.6 Importing User Assignments for Microsoft Exchange 2013/ 2016 / 2019

NOTICE: You can skip this configuration step if you have configured the user assignments via the Unified Communication templates in the CMP user management automatically.

You need to import the user assignments just created in OpenScape UC Application.

Start the configuration

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.

The dialog for importing a configuration opens.

- 4) In the **Import file** field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file.
- 5) Click on **Next**.
- 6) Check that the **Common Management Platform** option has been selected under **Type of file to be imported**.
- 7) Check that the **Domain Management** option has been selected under **Included type of data**.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

You have now imported the user assignments in OpenScape UC Application.

4.11.1.7 Configuring Access to Microsoft Outlook Contacts for Microsoft Exchange 2013/ 2016 / 2019

In order to store the personal contacts of the UC Application clients no longer in the OpenScape system, but in the contact folder of the Microsoft Exchange mailbox, you must configure the private contact lists of the OpenScape UC Application adequately.

IMPORTANT: If the contact management is migrated from the internal OpenScape-based solution to the Microsoft Exchange inbox, no contacts are synchronized that are already present in the OpenScape system.

Start the configuration

How to configure the access to Microsoft Outlook contacts:

- 1) Select in the CMP toolbar in the **Domain** combo box the domain for the users of which you want to configure the contact access.
- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click **Accounts > Contact Settings > Private List**.
A list of all private contact lists available in the OpenScape system is displayed in the workspace.
- 4) Select the check box of the **PrivateGroupwareContacts-Service** contact list.
- 5) Click **Set Default Contact Lists**.

OpenScape users are thus enabled to access Microsoft Outlook contacts in their UC Application client.

4.11.1.8 Configuring restricted Access to private Microsoft Exchange 2013/ 2016 / 2019 Contacts

You can configure the Microsoft Exchange connection also in such a way that the OpenScape users' access to their private Microsoft Exchange contacts is restricted to reading. How to proceed is described in [Configuring restricted Access to private Groupware Contacts](#) on page 443.

The Microsoft Exchange Server 2013/ 2016 / 2019 is now connected to OpenScape UC Application.

4.12 Connecting Microsoft Exchange Online

You can connect OpenScape UC Application to Microsoft Exchange Online.

The following sections describe the configuration steps that you need to execute for connecting the respective Microsoft Exchange Online system.

- [Configuring the Connection to Microsoft Exchange Online.](#)
- [Configuring Microsoft Exchange Online](#)
- [Configuring the OpenScape UC Application for the Connection with Microsoft Exchange Online](#)

4.12.1 Configuring the Connection to Microsoft Exchange Online

How to configure the Microsoft Exchange Online connection:

- 1) [Enabling the Multiline connector for Microsoft Exchange Online](#)
- 2) [Exporting Certificates for the AzureAD Configuration \(oAuth\)](#)

These steps are described in detail in the following sections.

4.12.1.1 Enabling the Multiline connector for Microsoft Exchange Online

NOTICE: This step is only necessary if more than one connector is required.

How to enable the Multiline connector:

- 1) Select Maintenance-> Inventory in the CMP.
- 2) Open the service list and find the Groupware Configuration Service.
- 3) Set the value of the parameter AllowMultiLine to true.

4) Restart the Groupware Configuration Service..

NOTICE: You can add more than one connectors to the groupware configuration if needed by following the same steps.

NOTICE: Additional connectors will appear as "new-
<longUUID>" in the service list. The SMTP configuration must be the same for all connectors.

4.12.1.2 Exporting Certificates for the AzureAD Configuration (oAuth)

Prerequisites

- A valid Exchange online subscription and an a matching ActiveDirectory Instance in Azure for the domain.
- An ExchangeOnline/ AzureAD tenant ID.

Step by step

NOTICE: You need to add the full path to the keytool when you want to run it on the OpenScape server. The Keytool is normally located in

```
/opt/siemens/share/ibm-java-<version>/jre/bin/  
keytool
```

1) To create a private key for the Backend:

- Open a shell on the application computer and switch to the directory in which the Java keytool is installed:

Under /opt/siemens/scs_groupware/conf/, specify the complete directory path that leads to the keytool:

```
/opt/siemens/share/ibm-java-<version>/jre/bin/keytool
```

NOTICE: Replace <version> with the correct Java version, e.g. /opt/siemens/share/ibm-java2-i386-60/jre/bin/keytool

- Execute the following lines in the relevant directory:

```
-genkey  
-keyalg RSA  
-alias selfsigned  
-keystore keystore.jks  
-storepass grppasswd  
-validity 360  
-keysize 2048
```

NOTICE: Use the same password for the key that was also used for the keystore.

2) Export the certificate in order to prepare the information for the AzureAD configuration:

- Open a shell on the application computer and switch to the directory in which the Java keytool is installed:

Under /opt/siemens/scs_groupware/conf/, specify the complete directory path that leads to the keytool:

/opt/siemens/share/ibm-java-<version>/jre/bin/keytool

NOTICE: Replace <version> with the correct Java version, e.g. /opt/siemens/share/ibm-java2-i386-60/jre/bin/keytool

- Execute the following lines in the relevant directory:

```
-exportcert
-alias selfsigned
-keypass grppasswd
-keystore keystore.jks
-storepass grppasswd
-rfc -file keytool_crtb64.der
```

Copy the keytool_crtb64.der to a windows machine where you can run a Powershell script.

Export the needed data via a Powershell script.

Example (getCertData.ps1):

```
$cerName = $args[0]
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import($cerName)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
Write-Output "Key-ID";
Write-Output $keyid;
Write-Output "Thumbprint";
Write-Output $base64Thumbprint;
Write-Output "Value";
Write-Output $base64Value;
```

- Execute the following line in the relevant directory by specifying the correct name and path of the keytool:

```
\getCertData.ps1
<NameAndPathofThekeytool_crtb64.de> >
certoutput.txt
```

You will get the following values in certoutput.txt:

- "Key-ID" (a random UUID),
- "Thumbprint" (the thumbprint of the certificate) and
- The raw value of the certificate ("Value").

- If you need to enable running unsigned Powershell script you can use the following command as administrator:

```
set-executionpolicy remotesign
```

Example:

Key-ID

```
72c26f30-e406-4ced-8d79-fa11146dc13e
```

Thumbprint

```
njP0gNUsbR3PD9h3SFRC3JMNuWY=
```

Value

```
MIIDRDCCAiygAwIBAgIEVQKcZDANBgkqhkiG9w0BAQUFADBkMQsw..
```

4.12.2 Configuring Microsoft Exchange Online

4.12.2.1 For previous version of Microsoft Azure Portal

- 1) Open the management portal of Azure,
- 2) Go to the ActiveDirectory instance of your Exchange Online Domain
- 3) Register a new app:
 - Search for UC_exchange_integration
 - Click Add.
 - Under section What do you want to do, select Add an application my organization is developing
 - Under section Tell us about your application, enter OpenScapeUC connector in the Name field and select Type Web Application or Web API.
 - Under section Application Properties, use the Openscape UC server URLs (they do not need to be accessible from the Internet).
 - Select Configure.
 - Note the CLIENT ID.
 - Under Permissions to other applications, click Add Application, and add Office 365 Exchange Online as application that needs to be accessed by the application.
 - Give the application the following permissions:
 - Office 365 Exchange Online: Application Permissions> "Have full access via EWS to all mailboxes in the..."
 - Windows Azure Active Directory: Application Permissions> "Read directory data"
 - Delegated Permissions: "Enable sign-on and read users' profiles"
 - Click Save.
- 4) Click Manage Manifest to download the manifest for the application.
 - Open the manifest in a text editor and change the section "keyCredentials" as follows (based on the example values from [Exporting Certificates for the AzureAD Configuration \(oAuth\)](#) on page 212:

```
"keyCredentials": [  
  {
```

```

"customKeyIdentifier": "<Thumbprint from
certoutput.txt>",
"keyId": "<KeyID from certoutput.txt>",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "<value from certoutput.txt>.."
}
],
Example:
"keyCredentials": [
{
"customKeyIdentifier": "njP0gNUsbR3PD9h3SFRc3JMNuWY=",
"keyId": "72c26f30-e406-4ced-8d79-fa11146dc13e",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "MIIDRDCCAiygAwIBAgIEVQKcZDANBgkqhkiG....."
}
],

```

- Save and upload the complete manifest again.
- You have configured Microsoft Exchange Online.

4.12.2.2 For new version of Microsoft Azure Portal

- 1) Open the management portal of Azure,
- 2) Go to the Azure Active Directory instance of your Exchange Online Domain
- 3) Register a new app:
 - Go to "App registrations", select "New application registration"
 - Enter <required name> in the Name field and select Type Web Application or Web API (Web app / API).
 - Under section "Sign-on URL", use the Openscape UC server URL e.g. <https://<server FQDN>> (no need to be accessible from the Internet).

4) Assign required permissions to the Application

- Under the UC Application settings, under "API ACCESS", click "Required permissions", then "Add", "Select an API" and select "Office 365 Exchange Online".
- Give the application the following permissions:

Select API "Office 365 Exchange Online", select permissions, under "Application Permissions", enable "Use Exchange Web Services with full access to all mailboxes".

Select API "Windows Azure Active Directory", under "Application Permissions", enable "Read directory data" and under "Delegated Permissions", enable "Sign in and read user profile".

For latest Azure versions (API Microsoft Graph) please follow the information below for step 4:

Assign required permissions to the Application:

- Under the UC Application settings, under "API Permissions", click "Add a permission", go to tab "APIs my organization uses", search for "office", select "Office 365 Exchange Online".
- Click "Application Permissions", enable "full_access_as_app".
- Click the "Add permissions" button at the bottom of the screen.
- Click "Add a permission" again.
- Select API "Microsoft Graph".
- Under "Application Permissions", enable "Directory.Read.All" and under "Delegated Permissions", enable "User.Read".
- Click the "Add permissions" button at the bottom of the screen.
- Click "Grant admin consent for <tenant name>" and click "yes" to confirm.

5) Get the necessary information for the UC Application Configuration:

- Click Manifest, and then download the manifest from the editor.

NOTICE: The browser editor can also be used to edit the manifest.

- Open the manifest in a text editor and change the section "keyCredentials" as follows (based on the example values from [Exporting Certificates for the AzureAD Configuration \(oAuth\)](#) on page 212

```
"keyCredentials": [  
  {  
    "customKeyIdentifier": "<Thumbprint from  
      certoutput.txt>",  
    "keyId": "<KeyID from certoutput.txt>",  
    "type": "AsymmetricX509Cert",  
    "usage": "Verify",  
    "value": "<value from certoutput.txt>.."  
  }  
],
```

Example:

```
"keyCredentials": [  
  {  
    "customKeyIdentifier": "njP0gNUsbR3PD9h3SFrc3JMNuWY=",
```

```

    "keyId": "72c26f30-e406-4ced-8d79-fa11146dc13e",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": "MIIDRDCCAiygAwIBAgIEVQKcZDANBgkqhkiG....."
  }
],

```

- Save and upload the complete manifest again.

You have configured Microsoft Exchange Online.

4.12.3 Configuring the OpenScape UC Application for the Connection with Microsoft Exchange Online

- 1) Click on the Inventory menu item on the Maintenance navigation tab of the CMP.
- 2) In the navigation tree, click on Nodes & Applications > Nodes.
A list of all system nodes and external links available in the entire system is displayed in the workspace.
- 3) Click on the name of the system node on which OpenScape UC Application is installed.
- 4) A dialog with the dashboard of the selected node opens.
- 5) Click on Show next to Actions – Show services status.
A dialog opens with a list of all components available for the selected system node. The State column displays whether the component is started or stopped.
- 6) Search the list for the Groupware SSL KeyManager component and click on the associated component name.
- 7) Change the value of property "certificateKeyStoreFilename" to "keystore.jks"

NOTICE: Copy the content from the "certificateKeyStorePassword" to the "certificateKeyStoreKeyPassword" entry

NOTICE: If you have other groupware connectors, be sure that all their certificates remain in the keystore.jks

NOTICE: You can use CTRL-A to really mark all in the certificateKeyStorePAssword field before copying the values, otherwise you might only copy a part.

- 8) Save and restart the service.

- 9) Create a Groupware Exchange Webservice connector and add the following configuration details:
 - Domain
This is the TenantDomain value as shown in AzureAD;
customersite.onmicrosoft.com
 - Technical user (can be any value).
 - Password (can be any value).
 - Exchange WebServices URL: `https://outlook.office365.com/EWS/Exchange.asmx`
 - SMTP configuration is the same as with a normal Exchange Server.
- 10) Click again on the Inventory menu item on the Maintenance navigation tab of the CMP.
- 11) In the navigation tree, click on Nodes & Applications > Nodes.
A list of all system nodes and external links available in the entire system is displayed in the workspace.
- 12) Click on the name of the system node on which OpenScape UC Application is installed.
- 13) A dialog with the dashboard of the selected node opens.
- 14) Click on Show next to Actions – Show services status.
- 15) Search for the Groupware Exchange Webservices SGDO backend provide or new* (in case of multiline the provider might show up as new-<UUID>).
- 16) Update the following configuration details:
 - exchange.auth.authprotocols
is "oAuth" (this is case sensitive).
 - **exchange.auth.domain**
is the TenantDomain value as configured on the Azure side. Can be found when connecting to AzureAD via PowerShell, using the AzureAD credentials for the specific UC connector.
 - exchange.auth.oauth.certThumbPrint
is the "customKeyIdentifier" value under "keyCredentials" found in the Azure manifest (json file) for this specific UC Connector.
 - exchange.auth.oauth.clientId
is the Application ID which can be found in the UC connector Registered app info page on the Azure portal. Can also be found as the value of "appld" in the Azure manifest (json file) for this specific UC connector.
 - **exchange.auth.oauth.keyalias**
What was used as an alias when creating the certificate (state preciously as "selfsigned").
 - exchange.auth.oauth.tenantID
is the TenantId value as configured on the Azure side. Can be found when connecting to AzureAD via PowerShell, using the AzureAD credentials for the specific UC connector.
 - exchange.auth.oauth.tokenGuid
is the "keyId" value under "keyCredentials" found in the Azure manifest (json file) for this specific UC connector.

- 17) If you need to use a proxy to connect to the Internet, enter the proxy server name in `exchange.auth.proxyname` and the port in `exchange.auth.proxyport`.

NOTICE: Proxy authentication is not supported.

- 18) Import the Office365 DigiCert into the UC Groupware keystore.

Go to <https://outlook.office365.com/EWS/Exchange.asmx> and export the DigiCert certificate.

Copy the exported cert file to the BE e.g. `/tmp/office365.crt` and execute:

```
"/opt/siemens/share/ibm-java-x86_64-71/jre/bin/keytool
-import -file /tmp/office365.crt -alias digikey -
keystore /opt/siemens/scs_groupware/conf/groupware.jks
-storepass grppasswd"
```

Then accept to "**Trust this certificate**" by typing "**yes**" and the Office365 certificate will be added into the UC Groupware keystore.

- 19) Import the DigiCert Baltimore CyberTrust Root certificate into the UC Groupware keystore.

Go to <https://baltimore-cybertrust-root.chain-demos.digicert.com/> and export the "Baltimore CyberTrust Root" certificate.

For the export the option "**Base-64 encoded X.509 (.CER)**" needs to be selected.

Copy the exported cert file to the BE e.g. `/tmp/Baltimore_CyberTrust_Root.cer` and execute:

```
"/opt/siemens/share/ibm-java-x86_64-71/jre/bin/keytool -
import -file /tmp/Baltimore_CyberTrust_Root.cer -alias
cybertrustroot -keystore /opt/siemens/scs_groupware/
conf/groupware.jks -storepass grppasswd"
```

Then accept to "**Trust this certificate**" by typing "**yes**" and the "Baltimore CyberTrust Root" certificate will be added into the UC Groupware keystore

NOTICE: If you are using the previous Azure AD Graph API (and not the latest Microsoft Graph API) you can verify that the appropriate permissions on the Office365/AzureAD side are enabled. For more details refer to step 3 under [For previous version of Microsoft Azure Portal](#) on page 214 or step 4 under [For new version of Microsoft Azure Portal](#) on page 215. On the Office365/AzureAD side apart from enabling all APPLICATION PERMISSIONS for both created APIs; "Windows Azure Active Directory" and "Office 365 Exchange Online", it is also necessary to allow/enable the DELEGATED PERMISSIONS for these two APIs.

- 20) Restart symphonica on the BE node.

You have configured the OpenScape UC Application for the connection with Microsoft Exchange Online.

4.12.4 Configuring an app in Azure AD for OpenScape UC Clients access to OL Local Contacts and Out of Office notification

- 1) Open the management portal of Azure.
- 2) Go to the Azure Active Directory instance of your Exchange Online Domain.
- 3) Select App Registrations, and then New registration.
- 4) Define a name for OpenScape UC application in MS Azure, for example "OpenScapeApp".
- 5) Select the account type your application is going to support, for example "Accounts in this organizational directory only".
- 6) Go to the registered application and select Authentication to add a new platform that will be used by WC, UC Desktop application and Fusion to access the info.
 - a) Adding a new platform for the Fusion Client:
 - Click on Add a platform.
 - Select the Mobile and Desktop applications platform.
 - Select the Redirect URI checkbox with: `https://login.microsoftonline.com/common/oauth2/nativeclient`
 - b) Adding a new platform for WebClient and UC Desktop App:
 - Click on Add a platform.
 - Select the single-page applications (SPA).
 - In the Redirect URIs field, fill the complete WC address (e.g.: `https://your-ucserver.net:8443/openscapeuc/`) and click "Configure". Other configurations available in this tab are not required.
 - Also add the Redirect URIs for each language that is supported by the UC Desktop Application, for example:
`https://your-ucserver.net:8443/openscapeuc/?language=en`
`https://your-ucserver.net:8443/openscapeuc/?language=de`
`https://your-ucserver.net:8443/openscapeuc/?language=fr`
`https://your-ucserver.net:8443/openscapeuc/?language=it`
`https://your-ucserver.net:8443/openscapeuc/?language=pt`
- 7) Select API Permissions, Microsoft APIs, and then the Microsoft Graph option. Select the Delegate permissions option as the type of permission.
- 8) Search for the permissions Contact.Read, Mail.Read, Mail.Read.Shared and User.Read and click the Add permissions button to add them. After this, use the "Grant admin consent..." button, to consent privileges in the tenant.
- 9) In Branding and properties session you can set the app image, change the name, etc.
- 10) The OpenScape Application is now configured in Azure AD of Office 365. In the app overview session, the administrator can get the Application (client) ID and the Directory (tenant) ID. These IDs must be copied to the WebClientUI.cfg file to allow OpenScape UC Clients to send valid requests to Office 365.

```
# Custom MS Azure application ID to use the  
# MS Graph API to retrieve MS Exchange data  
OpenScapeAPPID = your Application (client) ID
```



```
# MS Azure tenant ID to use the MS Graph API to
  retrieve
# MS Exchange data - used for single tenant mode.
# If empty multitenant is used (e.g., default: empty)
OpenScapeAPPTenantID = your Directory (tenant) ID
```

11) Feature activation in the UC Clients side:

MS Office 365 is now prepared and only requires the activation in the OpenScape UC Clients side to have access to the Out of Office notifications and Outlook Local Contacts.

Refer to the WebClient, UC Desktop App and Fusion Client User Guides for instructions on how to activate the integration for these Clients.

4.13 Synchronizing the MS Teams Presence with Openscape UC

The synchronization between MS Teams and OpenScape UC allows for changing the status of the MS Teams user to busy whenever the OpenScape UC presence status is set to busy as well. Whenever the status of the MS Teams user changes from busy to a different option, the previous status will be restored in OpenScape UC too. The opposite case will be also supported, thus, if the UC presence status is changed to busy then the MS Teams status will be changed as well.

Therefore, only the busy status of the Microsoft Teams user will be integrated into the OpenScape UC user presence status.

This is achieved by integrating the MS Graph interface in a new edge service and associating the MS teams account with the external id.

The table below displays when the MS Teams/OpenScape UC Presence changes to busy, when the user initiates a UC call:

Table 11: MS Teams/OpenScape UC Presence

MS Teams presence status prior to making a call	MS Teams presence status during a call
"availability": "Available", "activity": "Available",	"availability": "Busy", "activity": "Busy",
"availability": "Busy", "activity": "Busy",	"availability": "Busy", "activity": "Busy",
"availability": "DoNotDisturb", "activity": "DoNotDisturb",	"availability": "DoNotDisturb", "activity": "DoNotDisturb",
"availability": "BeRightBack", "activity": "BeRightBack",	"availability": "BeRightBack", "activity": "BeRightBack",
"availability": "Away", "activity": "Away",	"availability": "Away", "activity": "Away",
"availability": "Offline", "activity": "OffWork",	"availability": "Offline", "activity": "OffWork",

MS Teams presence status prior to making a call	MS Teams presence status during a call
"availability": "Busy", "activity": "InAMeeting",	"availability": "Busy", "activity": "Busy",

NOTICE: The user activity "InAMeeting" is fetched through Outlook synchronization, and it is shown when the user is not in a meeting call.

NOTICE: As per MS Teams API restriction, the subscription limit for MS teams users presence is limited to 650 users per technical user account.

4.13.1 Configuration in MS Azure Active Directory

Creation of the Azure application in Microsoft Azure Active Directory admin center:

- 1) To create an Azure application you need to login to Microsoft Azure Active Directory admin center with an administrator account and navigate to Azure Active Directory > Add > App Registration.
- 2) Perform a new Registration using the default settings to create an Azure application, as in the following example:
 - Application name: UCPresenceApp;
 - Accounts in this organizational directory only (Single tenant);
 - There is no need to define a Redirect URI.
- 3) Go to the Authentication option after selecting the newly created application. Set the Allow public client flows option to Yes.
- 4) Go to the Certificates & secrets section of the application and define a New client secret. Remember the value of the secret as it will not be available in the future. Please note that the client secret expires, therefore an update will be required before expiry.
- 5) Go to the API permissions section of the application and add the following permissions for the Microsoft Graph application:
 - Presence.Read.All for Delegated usage.
 - Presence.ReadWrite.All for Application usage.
 - User.Read.All for Application usage.

Admin consent will be required to apply the changes.

Admin consent					
User consent					
Search permissions					
API name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph (3)					
Microsoft Graph	Presence.ReadWrite.All	Read and write presence information for all users	Application	Admin consent	An administrator ...
Microsoft Graph	User.Read.All	Read all users' full profiles	Application	Admin consent	An administrator ...
Microsoft Graph	Presence.Read.All	Read presence information of all users in your o...	Delegated	Admin consent	An administrator ...

4.13.2 UC MS Graph Connector app in Facade node

- 1) Install the optional package for the UC MS Graph Connector app:

osc-setup up osc-setup

osc-setup in OpenScapeUC_Graph_Connector_Facade

- 2) Configure the UC Graph Connector in the Facade node.
- 3) Edit the file located under **/opt/uc-graph-connector/application.properties**
- 4) Fill in the following properties:

- **azure.activedirectory.clientId**: the application client id of your Azure registered application.
- **azure.activedirectory.tenantId**: the tenantId for your organization in Azure ADD.
- **azure.activedirectory.clientSecret**: the application client secret defined in your application that was registered in Azure.
- **azure.activedirectory.technical.user.username**: the username of the user that will be used as technical user to allow OpenScapeUC to use Microsoft Graph API.
- **azure.activedirectory.technical.user.password**: the password of the technical user.

Optional: support for more than one technical user (e.g. three technical users)

Since the Presence Subscription and Presence Read functionality are available only at Delegated Usage, only up to 650 users can be handled with one technical user.

To declare more technical users, add the following properties:

- **azure.activedirectory.technical.user.username.2**: the username of the second technical user
- **azure.activedirectory.technical.user.password.2**: the password of the second technical user
- **azure.activedirectory.technical.user.username.3**: the username of the third technical user
- **azure.activedirectory.technical.user.password.3**: the password of the third technical user

The definition of the first user is kept using the same properties (without a number) to achieve backwards compatibility with the existing functionality. The maximum number of technical users allowed is 25.

- **webhook.receiver**: the public URL in which UC Graph Connector can be accessed publicly and receive events from Microsoft Graph.

Example:

webhook.receiver = https://[Public_FQDN]:8443/graph/listen

- **webhook.listener.http.url**: the UC FE endpoint that point to the FE that will receive the events from UC Graph Connector and will propagate them

further to UC Backend. In case multiple FEs are defined they need to be comma separated.

Example:

```
webhook.listener.http.url = https:// [private_fqdn]:8443/owc-servlets/user/graph/notifications
```

For more information about how to configure TLS versions, ciphers and customer certificates, refer to [Configuring the Certificate for the UC Graph Connector](#).

4.13.3 Configuration of the callback uri in the HAProxy

The webhook.receiver public URL, used for Microsoft Graph event reception must be correspondingly configured in the reverse Proxy. For more information, refer to [Configuring HAProxy](#).

4.13.4 Configuration of UC Teams Graph Connector in UC BE

- 1) Navigate to the config beans directory in BE (/opt/siemens/common/conf/config-beans) and locate the config bean for the new OSGi bundle (displayName="Teams Connector Service"). The internal URL of façade node has to be defined in this config bean to allow the communication between Presence BE and Graph Connector in the Facade node.
- 2) Edit the GraphConnectorURL property, as the the example below:

```
<Property name="GraphConnectorURL" value="https://10.11.246.199:10443" writable="true"/>
```

NOTICE: Please note that here we use the internal IP address of the Graph Connector since they will communicate within the intranet. The definition of this property will be the triggering point that will indicate the busy (in a call) status needs to be synchronized between UC and MS Teams. If this value is empty, then the synchronization will not be possible, therefore this can be used as a way to temporarily disable the functionality, if needed.

- 3) Edit the MicrosoftTeamsExternalId property. It holds the name of the external Id that can be used in order to bind the UC users with the Azure AD users:

```
<Property name="MicrosoftTeamsExternalId" value="O365Teams" writable="true"/>
```

You should keep the default O365Teams value, unless there is a strong reason for changing it (e.g. the same external Id has been used for the definition of another integration).

- 4) It is also possible to define the delay in which the presence subscription process will be completed (e.g. fetch users via External Ids, retrieve their Azure AD id, subscribe for presence changes). By default, this action takes place 1 minute after the registration of the OSGi component. The delay can be adjusted according to specific requirements.

```
<Property name="GraphConnectorInitializationDelayMillis" value="60000" writable="true"/>
```

4.13.5 Startup and logs on the façade node

- 1) Start UC Graph Connector
`systemctl start uc-graph-connector`
- 2) Check status and logs of UC Graph Connector
`systemctl status uc-graph-connector`
`journalctl -f -u uc-graph-connector`
 log directory of graph connector: `/var/log/uc-graph-connector/`

4.13.6 User provisioning

To bind a UC user with an Azure user, you need to define the External Id for each user via CMP. This action needs to be performed for the users that need to have their busy presence status synchronized with the MS Teams status. The `assignedExternalSystemId` parameter should have the value `O365Teams` and the `externalId` should have the value of the `userPrincipal` name of the respective Azure user.

During the application startup, all the existing External IDs are retrieved. A presence subscription request is issued for the users with defined MS Teams external ids. Any newly defined external id definitions will be considered after the next application restart.

4.13.7 Administration of technical users and application secrets

To use the presence subscription method from the GraphAPI, you need to use a technical user account, since it is not allowed to use this functionality in Azure application level. This user does not need to have administrator privileges but should be a regular user created for the purpose of connecting OpenScapeUC with Microsoft Graph API.

To support more than 650 users, you need to set multiple technical users.

However, this approach may create some additional concerns for the management of the specific user account(s). More specifically, the administrators need to disable the MFA (Multi Factor Authentication) option for the specific user(s) in case there is a global setting that mandates the use of MFA. For more information, refer to:

<https://docs.microsoft.com/en-us/answers/questions/101179/how-to-disable-the-two-factor-authentication-from.html>

Furthermore, the administrators should mark the credentials of the specific user(s) to never expire. For more information, refer to:

<https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/set-password-to-never-expire?view=o365-worldwide>

If this is not possible (e.g. due to security concerns), then you should regularly check if password renewal must be performed and change the following properties:

- **azure.activedirectory.technical.user.password** property of the UC Graph Connector,

System Configuration

Configuring the IBM Lotus Domino Connection

- **azure.activedirectory.technical.user.password.(*)** property, if multiple technical users are used.

NOTICE: (*) indicates the number of additional technical user(s).

Apart from the credentials of technical user(s), the application client secret needs to be renewed before it expires. This currently represents an extra concern for the administrators, as in the past the client secrets did not have an expiration date. After creating a new application client secret, the administrator will have to update again the **azure.activedirectory.clientSecret** property of the UC Graph Connector.

4.14 Configuring the IBM Lotus Domino Connection

NOTICE: Special requirements must have been met for configuring the IBM Lotus Domino connection. See [Configuration Requirements](#) on page 80.

If you configure the IBM Lotus Domino connection, you cannot additionally connect any Microsoft Exchange version to the OpenScape system.

How to configure the IBM Lotus Notes connection at an IBM Lotus Domino 8.5.x or 9.0.x server:

- 1) [Creating a Linux User and Linux Group](#)
- 2) [Configuring the Connector Server](#)
- 3) [Stopping the Connector Server](#)
- 4) [Creating a technical User Account](#)
- 5) [Configuring Access Privileges for Mailboxes](#)
- 6) [Configuring Access Privileges for Files](#)
- 7) [Configuring the Groupware-Domino Connector](#)
- 8) [Configuring the IBM Lotus Notes System Configuration](#)
- 9) [Creating User Assignments/Importing User Assignments](#)
- 10) [Configuring Access to IBM Lotus Notes Contacts](#)
- 11) **If OpenScape Conference Extension for Lotus Notes is used:**
[Configuring the IBM Lotus Domino Server for OpenScape Conference Extension](#)

These steps are described in detail in the following sections.

You find continuative information about the technical design of the IBM Lotus Domino connection in [Configuring the IBM Lotus Domino Connection](#) on page 226.

4.14.1 Creating a Linux User and Linux Group

To install the connector server you need a Linux user and a Linux group.

Start the configuration

Create a Linux user and group by executing the steps of the following guide.

- 1) Start YaST.
- 2) Create a new user **notes** and assign him/her a password.
- 3) Create a new group **notes**.
- 4) Assign user **notes** to group **notes**.
- 5) Save the settings and close YaST.

You have now created a new Linux user and a new Linux group.

4.14.2 Configuring the Connector Server

NOTICE: To configure the connector server you need to execute the associated server setup. You can do that as remote server setup or via the Linux GUI. We recommend to use the remote server setup since the graphic user interface output of some Linux versions is problematic.

Before you install OpenScape UC Application you have set up the IBM Lotus Domino connector server on the computer system of OpenScape UC Application. To enable the groupware server accessing OpenScape UC Application via the Notes API of the connector server, you must configure the connector server.

Start the configuration

How to configure the connector server via the remote server setup:

NOTICE: If you use a firewall on the OpenScape UC Application computer system, you need to share port 8585 for inbound connections therein. The setup server listener for the remote server setup uses this port. After you have completely configured the IBM Lotus Domino connection, you can close this port in the firewall again.

Open a shell on the connector server computer system.

- 1) Log on under the user account you have previously created in [Creating a Linux User and Linux Group](#) on page 226 with the following command:

```
su <Name of the user account>
```

- 2) In the shell switch to the following path:

```
/local/notesdata
```

- 3) Execute the following command:

```
/opt/ibm/domino/bin/server -listen
```

The setup server listener starts on the IBM Lotus Domino server.

- 4) Select **Start > All Programs > Lotus Applications > Remote Server Setup** on the remote Windows computer.

NOTICE: If this feature is not installed on the remote Windows computer, install an IBM Lotus Notes client there and add this feature to the setup.

- 5) Specify the IP address under which the connector server can be reached.

The setup wizard starts.

- 6) Select **Next**.

The dialog for selecting the server type opens.

- 7) Select the **Set up the first server or a stand-alone server** option.

- 8) Select **Next**.

The dialog for specifying a server name and server title opens.

NOTICE: The connector server is exclusively used to establish the connection between the OpenScape system and the productive IBM Lotus Domino network. It is not integrated as IBM Lotus Domino server in the productive IBM Lotus Domino network. Therefore, you can arbitrarily select the name for the connector server. The only requirement is that you do not choose a name that is already used in the productive IBM Lotus Domino network.

- 9) Enter a server name and optionally a server title.

- 10) Select **Next**.

The dialog for entering the organization name opens.

- 11) Enter any organization name, a password and the password confirmation.

NOTICE: The entered password will not be needed for the following configuration steps.

- 12) Select **Next**.

The dialog for entering the IBM Lotus Domino domain name opens.

NOTICE: The connector server is exclusively used to establish the connection between the OpenScape system and the productive IBM Lotus Domino network. It is not integrated as IBM Lotus Domino server in the productive IBM Lotus Domino network. Therefore, you can arbitrarily select the domain name for the connector server. The only requirement is that you do not choose a name that is already used in the productive IBM Lotus Domino network.

- 13) Enter the IBM Lotus Domino domain name.

- 14) Select **Next**.

The dialog for entering the administration information opens.

- 15) Enter the name of the administrator, his/her password and the password confirmation.

NOTICE: The connector server is exclusively used to establish the connection between the OpenScape system and the productive IBM Lotus Domino network. It is not integrated as IBM Lotus Domino server in the productive IBM Lotus Domino network. You can therefore select default values for administrator name and password.

Example: Last Name = connectoradmin Password = Password1!

16) Select *Next*.

The dialog for selecting the internet services opens.

The settings in this dialog are not used by the IBM Lotus Domino connection.

17) Select *Next*.

The dialog for entering the network settings opens.

18) Verify that the displayed fully qualified domain name (FQDN) is correct for the server respectively customer network.

If a specification is incorrect, abort the process with **Cancel**. Then correct the fully qualified domain name under the following path.

Yast – Network Services – Routing and DNS

Leave the default values in this dialog otherwise unchanged.

19) Select *Next*.

The dialog for selecting the security settings opens.

Leave the default values in this dialog unchanged.

20) Select *Next*.

The dialog for creating an ID file opens.

Leave the default values in this dialog unchanged.

21) Select *Next*.

The dialog for confirming the entries opens.

22) If all settings are correct select *Setup*.

23) Select *Finish* when the setup is complete.

The dialog for stopping the setup server listener opens.

24) Select *Yes* to stop the setup server listener.

25) Restart the connector server with the following command for all initializations being performed automatically:

```
/opt/ibm/domino/bin/server
```

Launching the connector server may take some time. Therefore, wait until the outputs in the console log of the Domino server diminish.

You have now successfully configured the connector server.

4.14.3 Stopping the Connector Server

The IBM Lotus Domino connection only uses the Notes API installed on the set up connector server. The connector server itself is not required and must be stopped. This saves processing power on the OpenScape UC Application computer system.

Start the configuration

How to stop the connector server:

1) Go into the shell in which the connector server has been started and in which the console log of the Domino server is put out.

- 2) Execute the following command to stop the connector server:

```
exit
```

The connector server is stopped.

NOTICE: If you have closed the Domino console inadvertently, you can, as user notes, enter the following command in the /local/notesdata directory to stop the server from another console also: /opt/ibm/domino/bin/server -q

- 3) Enter the following command as root to check whether all processes were stopped:

```
ps -ef|grep notes
```

4.14.4 Creating a technical User Account

The Notes API on the OpenScape UC Application computer system uses a technical user account to connect to the groupware server. You need to create this user account on the groupware server.

Start the configuration

How to create the technical user account on the groupware server:

- 1) Start a Lotus administration client on the groupware server.
- 2) Register a new user.

Example: OscConnect

You have now created the technical user account.

4.14.5 Configuring Access Privileges for Mailboxes

OpenScape UC Application accesses the mail databases of the IBM Lotus Notes users via the technical user account. For this access it requires the corresponding access privileges on the groupware server.

Start the configuration

How to assign access privileges for mail databases to the technical user account:

- 1) Configure the following access privileges for the mail databases of the IBM Lotus Notes users on the groupware server for the technical user account.
 - Manager access
 - Delete documents
- 2) If you use roaming users under IBM Lotus Domino, configure for the technical user account the same privileges for the address books (names.nsf files) of the roaming users.

You have now assigned the required mailbox access privileges to the technical user account.

4.14.6 Configuring Access Privileges for Files

You have generated the files in the `/local/notesdata` directory of the connector server under the Linux user you have created in [Creating a Linux User and Linux Group](#) on page 226. But the Groupware-Domino connector accesses these files under the user **sym** of the group **sym**.

So that the IBM Lotus Domino connection works smoothly under these circumstances, you need to make the `/local/notesdata` directory and all files contained the property of user **sym** of the group **sym**.

NOTICE: After you have executed the following steps, you cannot start the connector server readily – neither under the Linux user *notes* nor under user **sym**.

Start the configuration

How to assign the `/local/notesdata` directory and all files contained therein to the **sym** user of the **sym** group:

- 1) Switch to the `/local` directory under Linux.
- 2) Enter the following command.

```
chown -R sym:sym notesdata
```

- 3) Use the following command to check whether the modification was correctly performed:

```
ls -l notesdata -rw-r--r--1 sym sym 327680 Jan28 14:35
AgentRunner.nsf -rw-r--r--1 sym sym 0Jan 28 14:42
DDMRepCach.dat
```

You have now assigned the `/local/notesdata` directory and all files contained therein to user **sym** of the **sym** group.

4.14.7 Configuring the Groupware-Domino Connector

OpenScape UC Application is connected to the IBM Lotus Domino server via the Groupware-Domino connector. To this, configure in the Groupware-Domino connector how it accesses the IBM Lotus Domino server.

Start the configuration

How to configure the Groupware-Domino connector:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select **Add**.

The dialog for adding a new groupware connection opens.

- 5) Select the **Lotus Notes** entry under **Connection Type**.

- 6) Specify a unique identifier for the connection under **Connection ID**.

Example: ConnectionLN

You will later use this identifier to assign this connection to OpenScape users.

- 7) Select **Save**.

The new connection is displayed in the list of all configured groupware connections.

- 8) Select the radio button of the connection you have just added.

- 9) Select **Configure**.

The configuration dialog of the selected connection opens.

- 10) Enter under **Description** a short description for the connection.

- 11) Specify the name of an IBM Lotus Domino directory server under **Domino Directory Server**. In doing so, use canonical notation.

Example: CN=Domino/OU=Doc/O=Org/C=DE

- 12) Specify the e-mail address of the technical user account under **Default Sender Address**.

This address is used as originator address for e-mails that OpenScape UC Application sends automatically. OpenScape UC Application sends non-delivery reports to this address also.

- 13) Select **Save**.

The configuration dialog closes and the settings are saved.

You have thus configured the Groupware-Domino connector.

4.14.8 Configuring the IBM Lotus Notes System Configuration

The Notes API on the OpenScape UC Application computer system uses a technical user account to connect to the groupware server. You have created this user account on the groupware server in a previous section.

You need to perform various settings for the Notes API to connect to the groupware server via this user account.

Start the configuration

Perform the IBM Lotus Notes system configuration by proceeding in the configuration dialogs of all configured groupware connections as follows.

- 1) In the dialog of the configured groupware connections switch to the **Lotus Notes System Configuration** tab.
- 2) Select under **Lotus Notes User** in the **Lotus Notes ID File** field the ID file that was generated when creating the technical user account. Use **Browse** for this purpose.
- 3) Enter the password for the technical user account under **Password**.
- 4) To activate the new user ID, select **Change User ID**.
- 5) Select under **Domino Server Connections** the **Add** button for specifying in succession all IBM Lotus Domino servers on which the mail databases are

managed. Also specify the IBM Lotus Domino directory server you specified on the **Connection Configuration** tab.

A new entry is added to the connection list. Define the following settings in this entry.

- a) Enter the name of the relevant IBM Lotus Domino server in the **Domino Server Name** field. In doing so, use hierarchical notation.

Example: dominoServer1/orgUnit1/Org1

NOTICE: You can look for the server name in the Domino directory.

- b) Enter under **Domino Server Address** the IP address of the computer system on which the specified IBM Lotus Domino server is installed.

If the host name of the computer system can be resolved into an IP address via a DNS server, you can also enter the associated host name instead of the IP address.

- 6) Select **Activate Server Connections** for applying the performed settings.

You have thus configured the IBM Lotus Notes system configuration.

4.14.9 Creating User Assignments

To ensure a smoothly operating IBM Lotus Domino connection, you need to assign the respectively associated IBM Lotus Domino user account to the relevant OpenScape user accounts. In addition, you need to specify for the voice portal which IBM Lotus Domino e-mail account belongs to an OpenScape user account. Import the corresponding user assignments in OpenScape UC Application for this purpose.

Before you can import the user assignments in OpenScape UC Application you need to create the relevant assignments.

NOTICE: Only the user assignments that the relevant users require are exported in the following. This assumes the contact information having already been specified in OpenScape UC Application.

Start the configuration

How to create the user assignments:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.

The dialog for exporting configurations opens.

- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.
- 8) Open the downloaded Zip file and open the following Zip file contained therein:

```
${exportWorkingDir}\  
Package_domainmanagement_domainmanagement001.zip
```

- 9) In there open the following file with a text editor:

```
${BackupAppWorkDir}\domain_configuration.csv
```

NOTICE: If the data is to contain special characters, you need to use a text editor that supports the UTF-8 file format. Microsoft Windows Wordpad and Microsoft Word do not support the UTF-8 file format. Notepad does.

NOTICE: The text editor used must not deploy a Byte-Order-Mark – BOM.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the user assignments under the entry that begins with `##ExternalId`.
 - The fields of an entry are separated from each other by semicolon.
- 10) Look for the user assignments section in the file. This section begins with the following line:

```
##ExternalId;externalId;isContactMaster ...
```

- 11) Remove all lines that do not belong to the user assignments section from the file.

In a file without existing user assignment, only the following line then remains:

```
##ExternalId;externalId;isContactMaster ...
```

- 12) In the exported file `domain_configuration.csv` under `##ExternalId` add all required user assignments that assign the respectively associated

IBM Lotus Domino e-mail account to the relevant OpenScape user accounts.

In doing so please note:

- The following data special characters must be marked by the escape character \ for later import: , \ # =
- Create for each assignment of OpenScape user account and IBM Lotus Domino user account a new ExternalId entry.

How to specify the data for a new user assignment:

- a)** Enter the reserved name **ExternalId** in the user entry under **##ExternalId**.

This name defines the entry as user assignment.

NOTICE: The ExternalID can be also modified in corresponding ExternalID tab in CMP

- b)** Specify under **externalId** a name that is unique for all ExternalId entries in the OpenScape system.

For example, use the e-mail address of the associated user or number the entries consecutively.

- c)** Always specify the **false** value under **isContactMaster**.

- d)** Always specify the **false** value under **isProvisioningMaster**.

- e)** Specify under **assignedExternalSystemId** the unique name you have determined in the **Logical connection** field of the Groupware-Domino connector (cf. [Configuring the Groupware-Domino Connector](#) on page 231).

- f)** Specify under **additionalInfo** the following information and separate it with a comma:

- Groupware_Mailbox:
<Name of the IBM Lotus Notes user in canonical format>
- Groupware_Address:
<E-mail address of the IBM Lotus Notes user>
- GwType:
Notes

- g)** Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: mSample@system

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	isContactMaster	isProvisioningMaster	...
ExternalId	1	false	false	...
ExternalId	2	false	false	...

System Configuration

##ExternalId	externalId	isContactMaster	isProvisioningMaster	...
...	...	...	...	...

additionalInfo
Groupware_Mailbox:CN=mSample/OU=Doku/O=Company/ C=DE,Groupware_Address:mSample@co.com,GwType:notes
Groupware_Mailbox:CN=tBrown/OU=Doku/O=Company/ C=DE,Groupware_Address:tBrown@co.com,GwType:notes
...

...	assignedExternalSystemId	assignedUserIdentity
...	ConnectionLN	mSample@system
...	ConnectionLN	tBrown@system
...	...	...

```
##ExternalId;externalId;isContactMaster;isProvisioningMaster;additionalInfo;assignedExternalSystemId;assignedUserIdentity
ExternalId;1;false;false;Groupware_Mailbox:CN=mSample/OU=Doku/O=Company/C=DE,Groupware_Address:mSample@co.com,GwType:notes;ConnectionLN;mSample@system
ExternalId;2;false;false;Groupware_Mailbox:CN=tBrown/OU=Doku/O=Company/C=DE,Groupware_Address:tBrown@co.com,GwType:notes;ConnectionLN;tBrown@system
...
```

- 13)** In the exported file `domain_configuration.csv` under `##ExternalId` add all required user assignments that assign the respectively associated

IBM Lotus Domino e-mail account to the relevant OpenScape user accounts. This assignment is required for the voice portal.

Please note: Create for each assignment of OpenScape user account and IBM Lotus Domino e-mail account a new ExternalId entry.

How to specify the data for a new user assignment:

- a) Enter the reserved name **ExternalId** in the user entry under **##ExternalId**.

This name defines the entry as user assignment.

NOTICE: The ExternalID can be also modified in corresponding ExternalID tab in CMP

- b) Specify under **externalId** the unique IBM Lotus Domino e-mail account of the relevant OpenScape user.
- c) Always specify the **false** value under **isContactMaster**.
- d) Always specify the **false** value under **isProvisioningMaster**.
- e) Always specify the **Groupware_Domain** value under **assignedExternalSystemId**.
- f) Do not specify a value under **additionalInfo**.
- g) Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: mSample@system

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	isContactMaster	isProvisioningMaster	...
ExternalId	mSample@co.com	false	false	...
ExternalId	tBrown@co.com	false	false	...
...	...	...	...	...

additionalInfo	...	assignedExternalSystemId	assignedUserIdentity
	...	Groupware_Domain	mSample@system
	...	Groupware_Domain	tBrown@system

System Configuration

additionalInfo	...	assignedExternalSystemId	assignedUserIdentity
...	...	...	...

```
##ExternalId;externalId;isContactMaster;  
isProvisioningMaster;additionalInfo;assignedExternalSystemId;  
assignedUserIdentity  
ExternalId;mSample@co.com;false;false;;  
Groupware_Domain;mSample@system  
ExternalId;tBrown@co.com;false;false;;  
Groupware_Domain;tBrown@system  
...
```

- 14) Save the supplemented file `domain_configuration.csv` in the CSV format.

IMPORTANT: If the data contain special characters, you need to store the file in the UTF-8 file format also.

- 15) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

You have now created the required user assignments.

4.14.10 Importing User Assignments

You need to import the user assignments just created in OpenScape UC Application.

Start the configuration

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.
The dialog for importing a configuration opens.
- 4) In the **Import file** field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file.
- 5) Click on **Next**.
- 6) Select under **Type of file to be imported** the **Common Management Platform** entry.
- 7) Select under **Included type of data** the **Domain Management** entry.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

4.14.11 Configuring Access to IBM Lotus Notes Contacts

So that OpenScape users can access their IBM Lotus Notes contacts in their UC Application client, you need to configure the private contact lists of OpenScape UC Application accordingly.

Start the configuration

How to configure the access to IBM Lotus Notes contacts:

- 1) Select in the CMP toolbar in the **Domain** combo box the domain for the users of which you want to configure the contact access.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click **Accounts > Contact Settings > Private List** .
A list of all private contact lists available in the OpenScape system is displayed in the workspace.
- 4) Select the checkbox of the **PrivateGroupwareContacts-Service** contact list.
- 5) Click **Set Default Contact Lists**.

OpenScape users are thus enabled to access their IBM Lotus Notes contacts in their UC Application client.

The IBM Lotus Domino server is now connected to OpenScape UC Application.

NOTICE: You find detailed information about logging the Groupware-Domino connector in [Logging the Groupware Service](#) on page 618.

4.14.12 Configuring the IBM Lotus Domino Server for OpenScape Conference Extension

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Conference Extension for - Lotus Notes.

Using OpenScape Conference Extension for Lotus Notes requires configuring the IBM Lotus Domino server appropriately. For this purpose, the template database `osconf.ntf` is shipped with OpenScape UC Application. This template database contains all database elements that, in the scope of the following configuration, need to be copied into the mail template database of the IBM Lotus Notes users who are to deploy OpenScape Conference Extension for Lotus Notes.

NOTICE: Please note that the default language in the template database `osconf.ntf` is British English. Consequently, this is

the default language for the components you will copy from the template database to your mail template database. Therefore, do not mix such components with other components of another default language.

Configuring the IBM Lotus Domino server for OpenScape Conference - Extension for Lotus Notes stretches over the following sections:

- 1) [Dividing a multilingual Mail Template](#)
- 2) [Preparing the Configuration](#)
- 3) [Copying Images into the Mail Template Database](#)
- 4) [Copying Script Libraries into the Mail Template Database](#)
- 5) [Copying Form Actions into the Mail Template Database](#)
- 6) [Changing the Forms' Code](#)
- 7) [Creating a Configuration Button for Conferences](#)
- 8) [Configuring the Activation of the Presence Plugin Thread](#)
- 9) [Configuring the Deletion of Conferences](#)
- 10) [Activating the Configuration for IBM Lotus Notes Users](#)

IMPORTANT: Execute the instructions in these sections precisely in the given sequence.

The configuration steps an IBM Lotus Notes user then still needs to perform in his/her IBM Lotus Notes client are described in the operating instructions *OpenScape UC Application Client Applications*.

Requirements for the following configuration

The following configuration is based on various system components and requirements:

- IBM Lotus Notes Client
- IBM Lotus Domino Designer
- The template database `osconf.ntf` of OpenScape UC Application.

You find this template database on the first setup DVD in the archive:

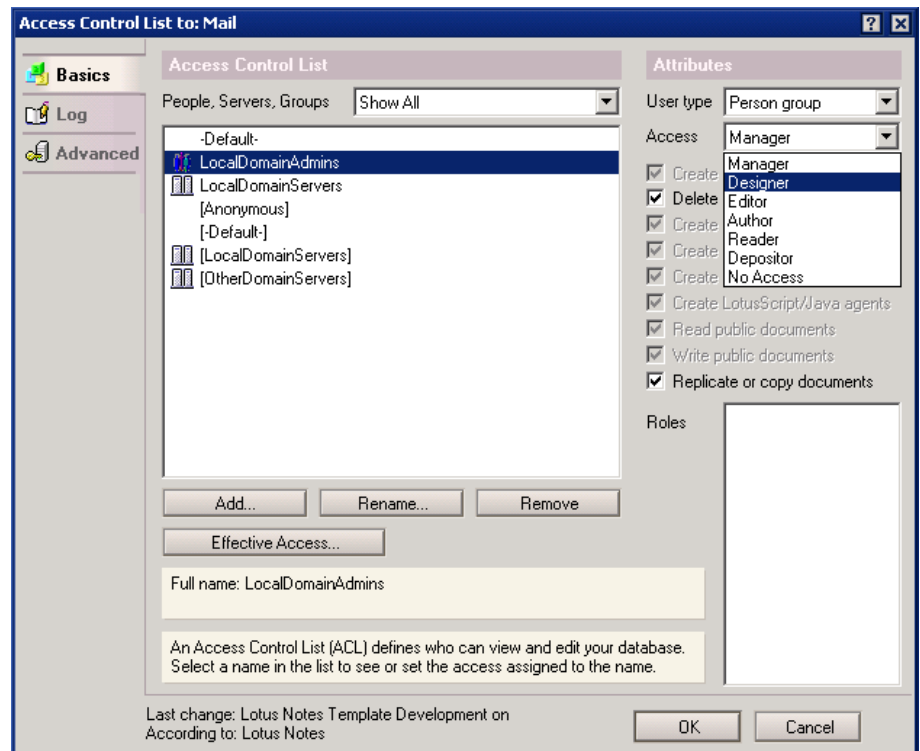
`/win32/OpenScapeExtensionsForLotusNotes-<version>.zip`

- For step [4 on page 482](#) you need to be logged in as Lotus Domino administrator.
- At least developer privileges that allow access to the template database `osconf.ntf` and the mail template database of the IBM Lotus Notes users.

You can modify the access privileges in the access control list (ACL) of the respective database. A click on a database in the IBM Lotus Notes client

workspace with the right mouse button and selecting **Application > Access Control ...** opens the access control list of this database.

NOTICE: The file name of the mail template database is typically mail8.ntf, the title is Mail (R8) and the template name StdR8Mail.



For the persons, servers and groups displayed in the field on the left hand side you can set the access privileges in the **Access** field and in the check boxes thereunder.

4.14.12.1 Dividing a multilingual Mail Template

NOTICE: You need to execute the configuration steps of this chapter only if you use multilingual mail templates in your IBM Lotus Domino server.

The configuration described in the following sections does not support any multilingual mail templates. If you use such a mail template in your IBM Lotus Domino server, you need to divide it into different, language-specific mail templates first.

Start the configuration

How to divide a multilingual mail template in different language-dependent mail templates:

- 1) Start the IBM Lotus Domino Designer on a computer from which you can access the IBM Lotus Domino server that hosts the multilingual mail template.
- 2) Select the **File > Application > New** menu option.
The dialog for creating a new application opens.
- 3) Select under **Server** the server on which you wish to store the new language-dependent mail template.
- 4) Specify a title for the new language-dependent mail template under **Title**.
- 5) The file name under **File name** is created automatically. Change the name prefix to .ntf.
- 6) Select the multilanguage mail template under **Specify Template for New Application**.
- 7) Disable the **Inherit future design changes** option.
- 8) Select **OK**.
A dialog in which you can select the language for the newly created mail template opens.
- 9) Select exactly one language for the newly created mail template.
- 10) Open **Application Properties** for the newly created mail template and switch to the **Design** tab.
- 11) Enable the **Database file is master template** option.
- 12) Enter a name for the template under **Template name**.
- 13) Execute the outlined steps for all required languages.

4.14.12.2 Preparing the Configuration

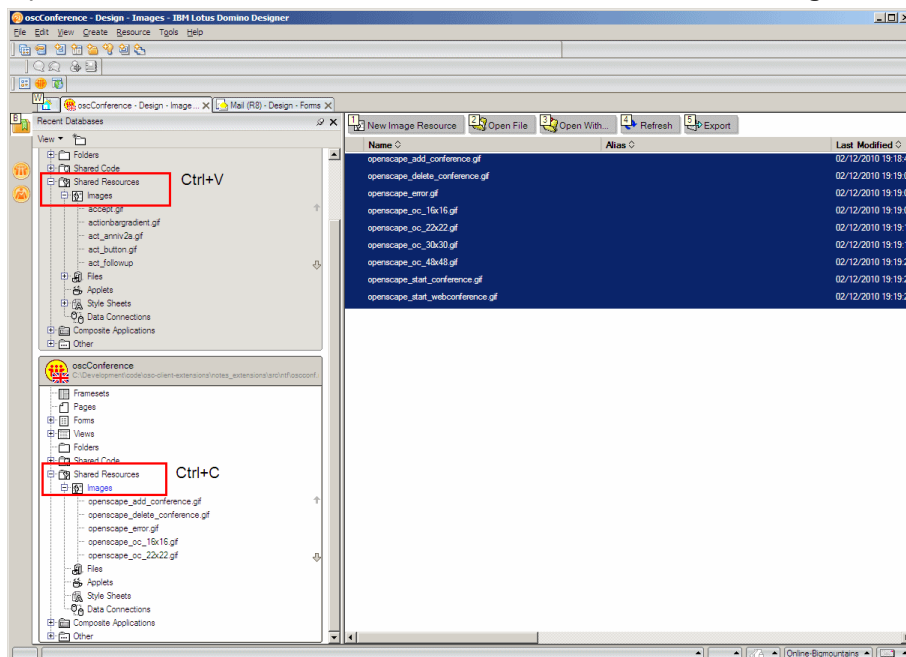
How to prepare the configuration:

- 1) Create a backup copy of the mail template database.
- 2) Start the IBM Lotus Domino Designer on a computer from which you can access the template database `osconf.ntf` and the IBM Lotus Domino server that hosts the mail template databases of the IBM Lotus Notes users.
- 3) Open the `osconf.ntf` file in the IBM Lotus Domino Designer.

4.14.12.3 Copying Images into the Mail Template Database

How to copy images from the `osconf.ntf` file into the mail template database:

- 1) Open in the oscconf . ntf file the folder **Shared Resources > Images**.

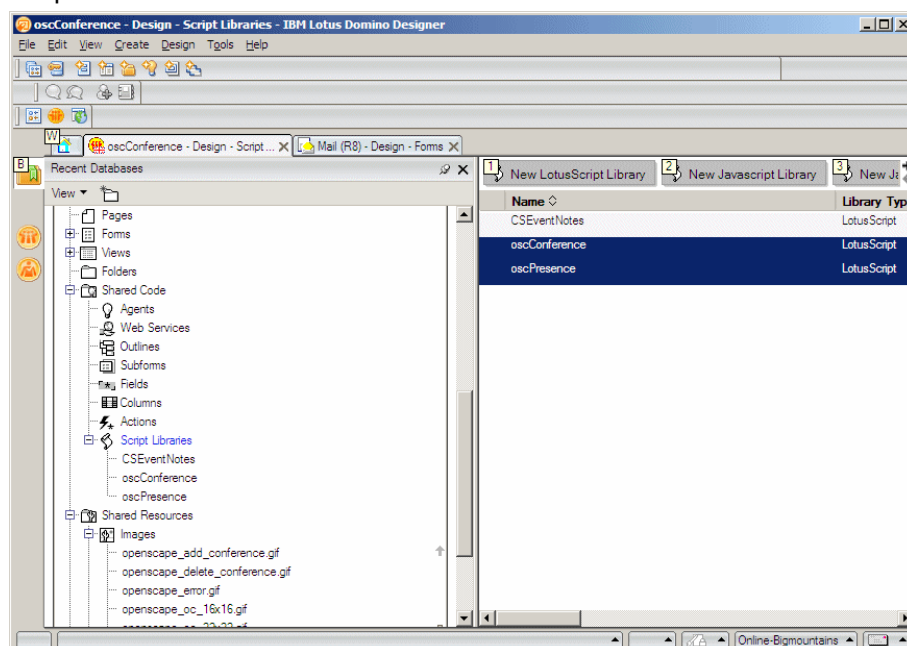


- 2) Copy all images available in this folder to the clipboard.
- 3) Open the original mail template database in the IBM Lotus Domino Designer. Open **Shared Resources > Images** in there as well.
- 4) Paste the content of the clipboard.

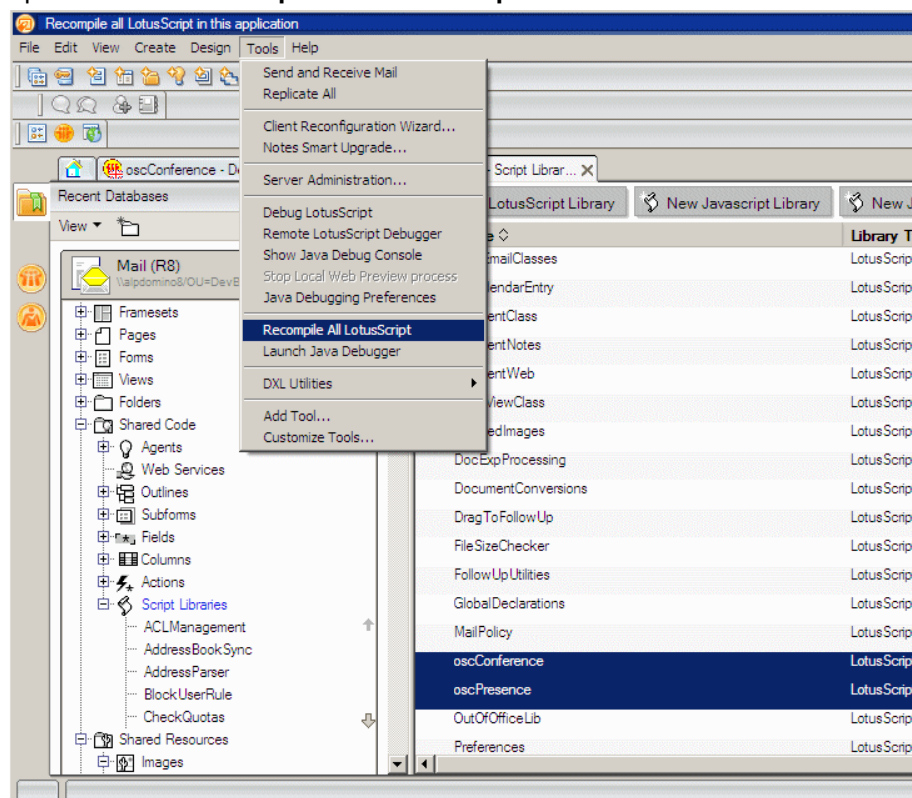
4.14.12.4 Copying Script Libraries into the Mail Template Database

How to copy script libraries from the oscconf . ntf file into the mail template database and recompile and sign these:

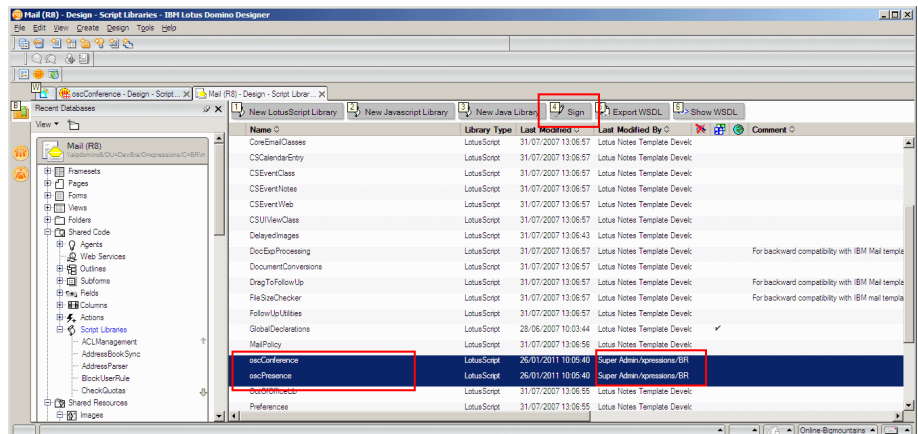
- 1) Copy the script libraries **oscConference** and **oscPresence** from the folder **Shared Code > Script Libraries** of the **osconf.nsf** file into the mail template database.



- 2) Recompile in the mail template database all scripts by selecting the menu option **Tools > Recompile All LotusScript**.



- 3) Select in the mail template database the two script libraries **oscConference** and **oscPresence**.



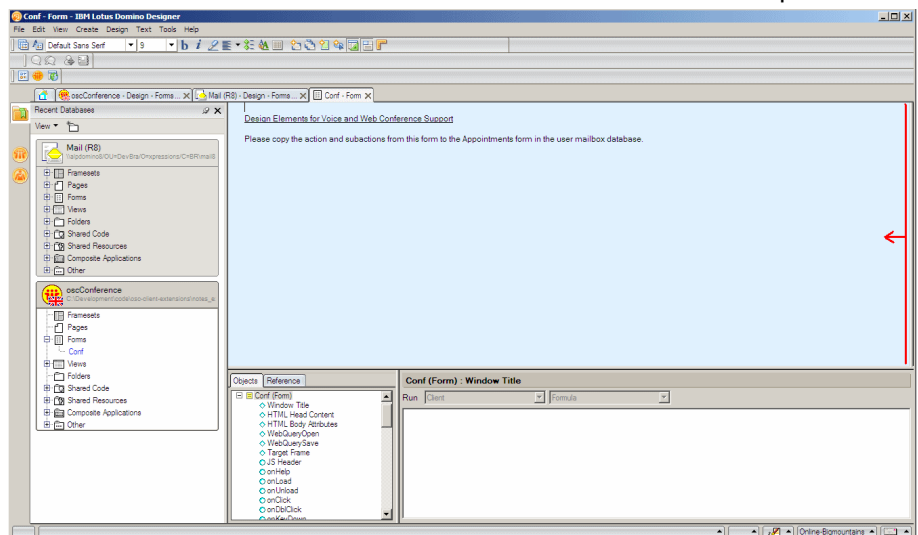
- 4) Click the **Sign** button.

NOTICE: Be sure to execute this step as Lotus Domino administrator.

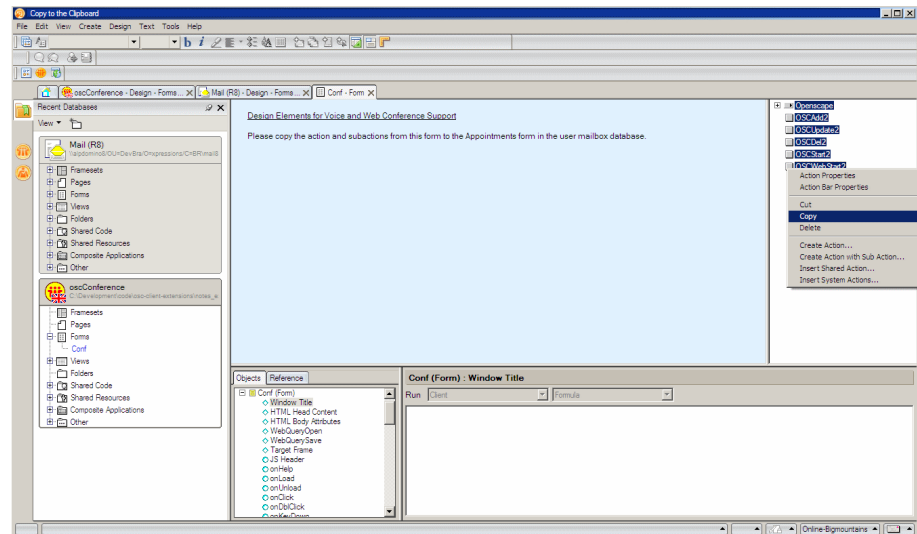
4.14.12.5 Copying Form Actions into the Mail Template Database

How to copy actions of a form from the `osconf.ntf` file into the mail template database:

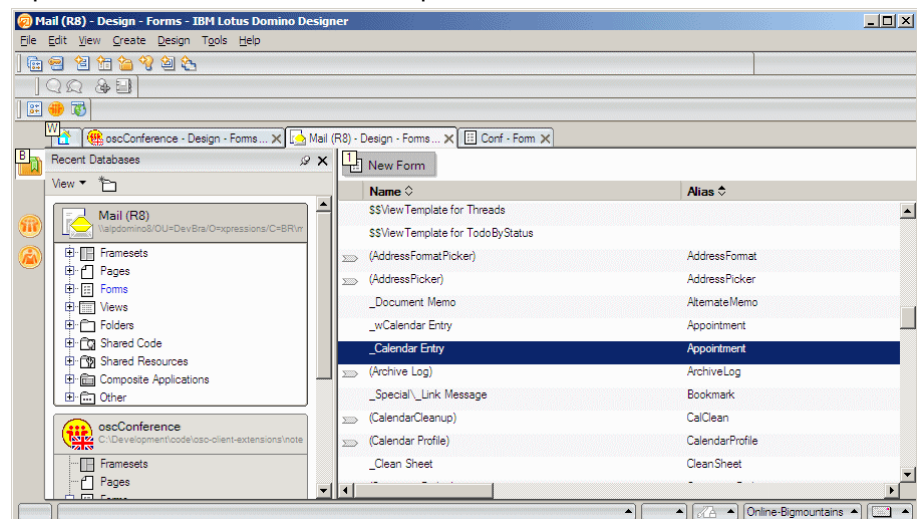
- 1) Doubleclick in the `osconf.ntf` file the form **Forms > Conf** to open it.



- 2) Activate the checkbox of the menu option **View > Action Pane** or drag the right boundary line of the form to the left for displaying the actions.



- 3) Select all actions in the action pane with the right mouse button and select **Copy**.
- 4) Open the **Forms** folder in mail template database.



- 5) Click on the **Alias** column caption to sort according to this column. Doubleclick the entry that has value **Appointment** in the **Alias** column and one of the following values in the **Name** column:

- German: **_Kalendereintrag**
- English: **_Calendar Entry**
- French: **_Entrée d'agenda**
- Italian: **Vo_ce del diario**
- Spanish: **E_ntrada de agenda**
- Portuguese (Portugal): **_Entrada da agenda**
- Portuguese (Brazil): **Entrada na_Agenda**
- Dutch: **_Agenda-item**

Select the language the user deploys in the IBM Lotus Notes client.

IMPORTANT: Do not click the entry that has the **_wCalendar Entry** value in the **Name** column.

- 6) Activate the checkbox of the menu option **View > Action Pane** or drag the right boundary line of the form to the left for displaying the actions.
- 7) Click in the action pane.

The topmost action is selected automatically.

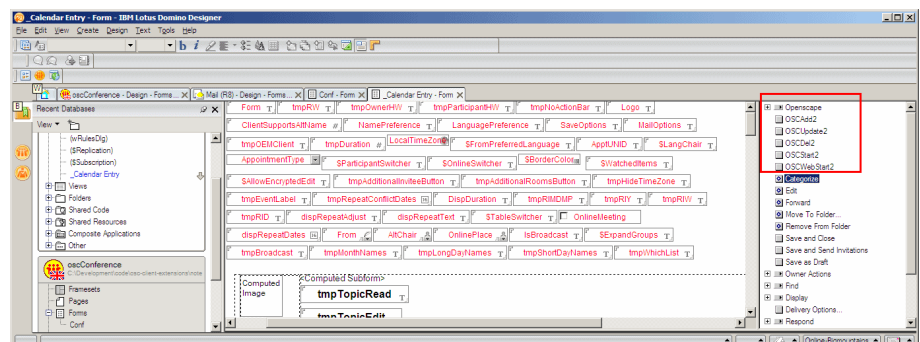
- 8) Paste the content of the clipboard.

The actions from the clipboard are pasted under the action topmost so far.

- 9) Click with the left mouse button on the just pasted actions, keep the mouse button pressed, drag the mouse over the topmost action and release the mousebutton again.

The selected actions are now in topmost position.

NOTICE: This step is not necessary but recommended.



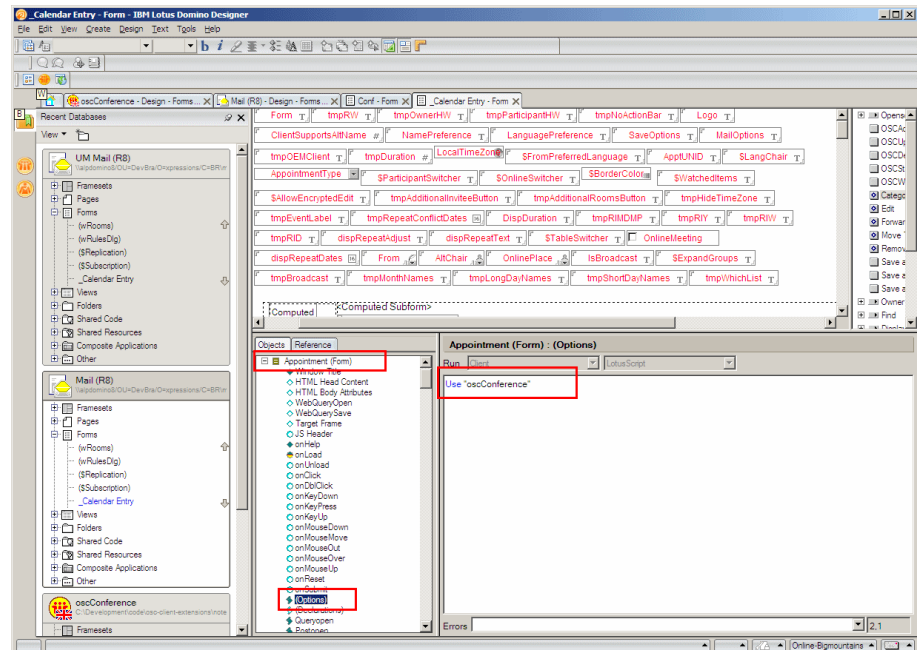
4.14.12.6 Changing the Forms' Code

NOTICE: Configuring this section effects an automated update when the user changes a conference's properties but does not click on the **Update Conference** button before saving the conference.

How to change the code in specific areas of the form:

- 1) Click on the **Objects** tab underneath the form.
- 2) Select **Appointment (Form) > (Options)**.
- 3) Enter the following code in section **Appointment (Form) : (Options)** on the right hand side:

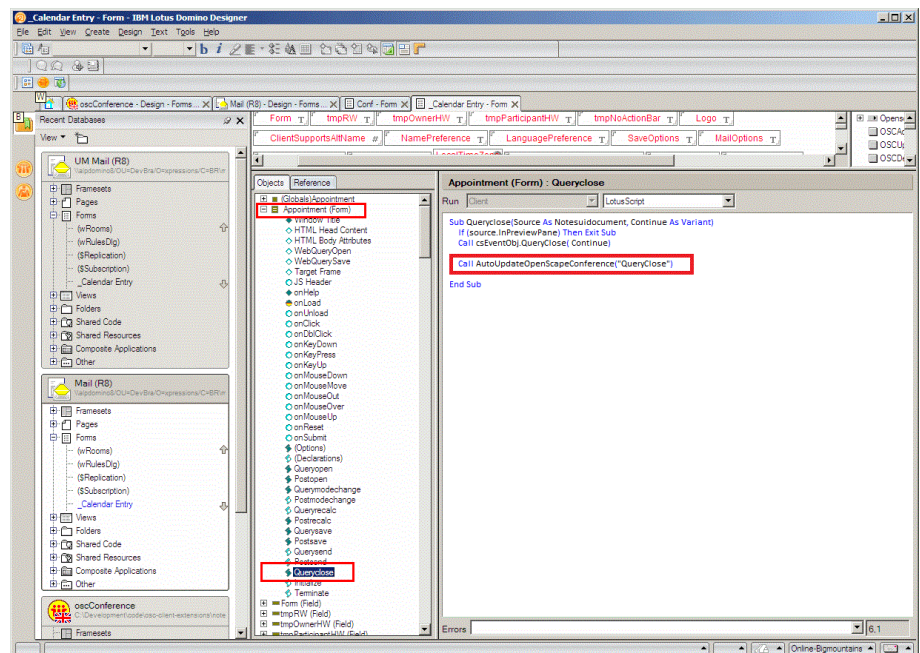
Use "oscConference"



- 4) Click on the **Objects** tab underneath the form and select **Appointment (Form) > Queryclose**.

Code is automatically created in the **Appointment (Form) : Queryclose** section.

- 5) Look for the following code line in this code:
End Sub
- 6) Paste the following line before this code line:
Call AutoUpdateOpenScapeConference ("QueryClose")



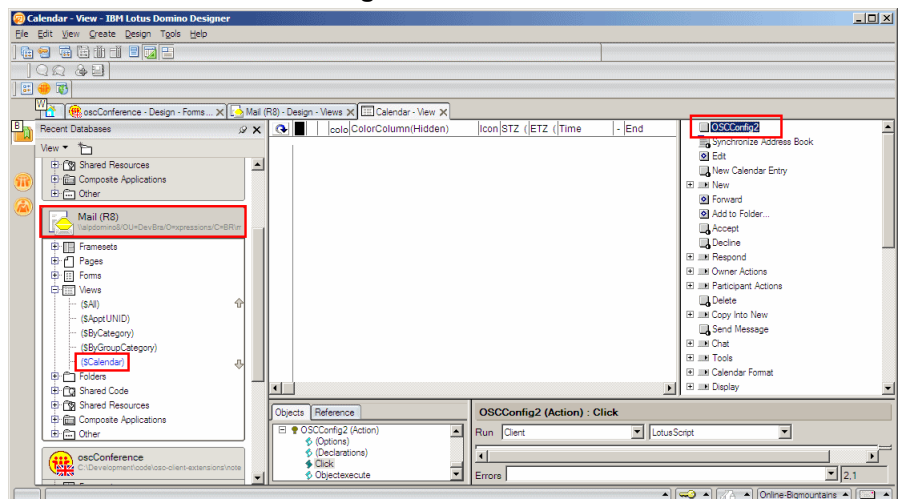
7) Save the form and close it.

4.14.12.7 Creating a Configuration Button for Conferences

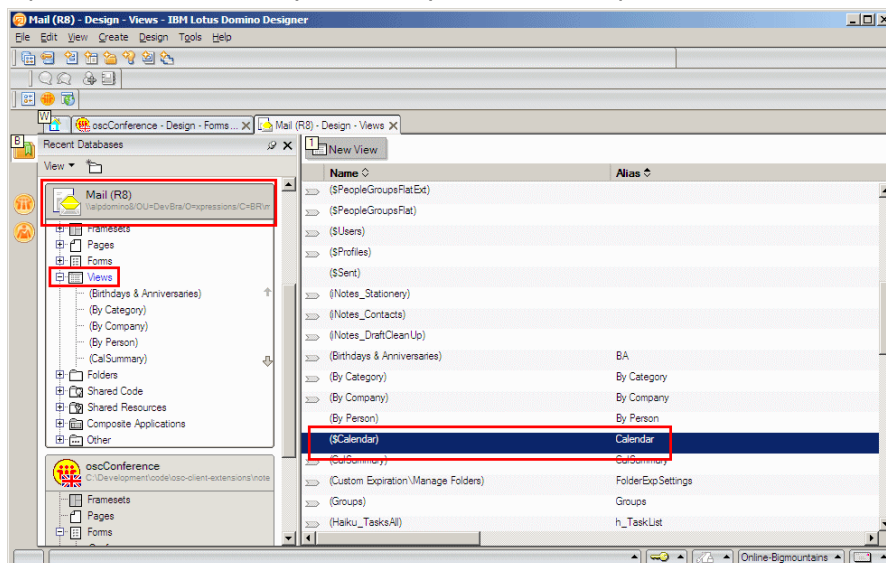
NOTICE: The configuration of this section is optional because it is already available in a meeting form.

How to create a configuration button for conferences in the calendar view:

- 1) Open in the `osccnf . n t f` file in the IBM Lotus Notes Designer the view **Views > (\$Calendar)**.
- 2) Activate the check box of the menu option **View > Action Pane** or drag the right boundary line of the form to the left for displaying the actions.
- 3) Click in the action pane.
- 4) Click on the action **OSCCfg2**.

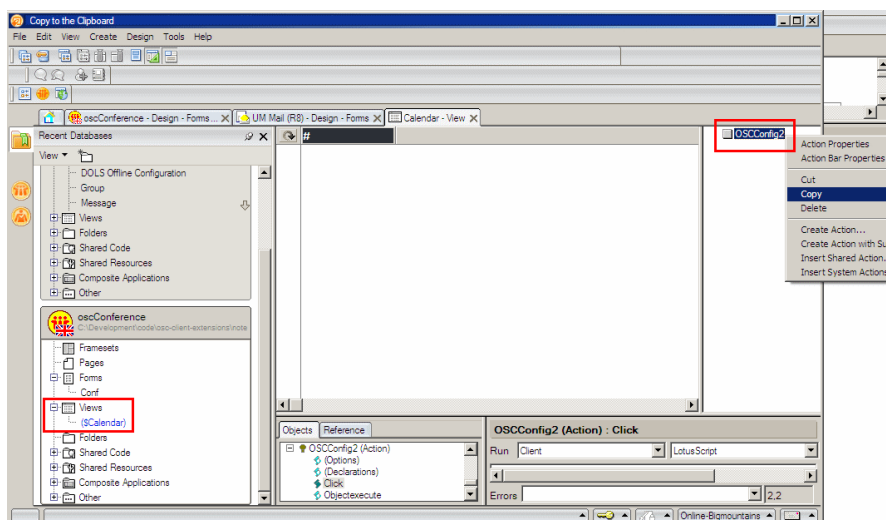


- 5) Copy it to the clipboard.
- 6) Open the view **Views > (\$Calendar)** in the mail template database.



- 7) Activate the check box of the menu option **View > Action Pane** or drag the right boundary line of the form to the left for displaying the actions.
- 8) Click in the action pane.
The topmost action is selected.
- 9) Paste the clipboard.
The actions from the clipboard are pasted under the action topmost so far.
- 10) Click with the left mouse button on the just pasted action, keep the mouse button pressed, drag the mouse over the topmost action and release the mousebutton again.
The selected action is now in top position.

NOTICE: This step is not necessary but recommended.

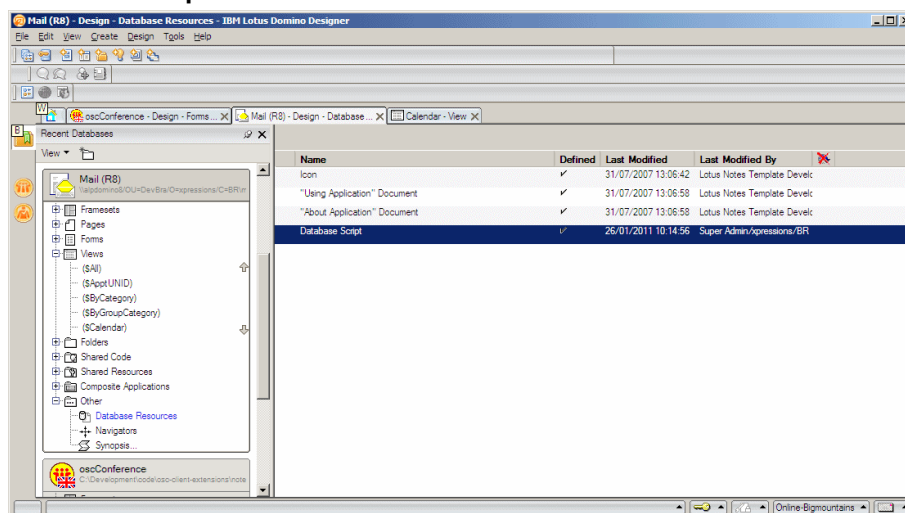


- 11) Save the view and close it.

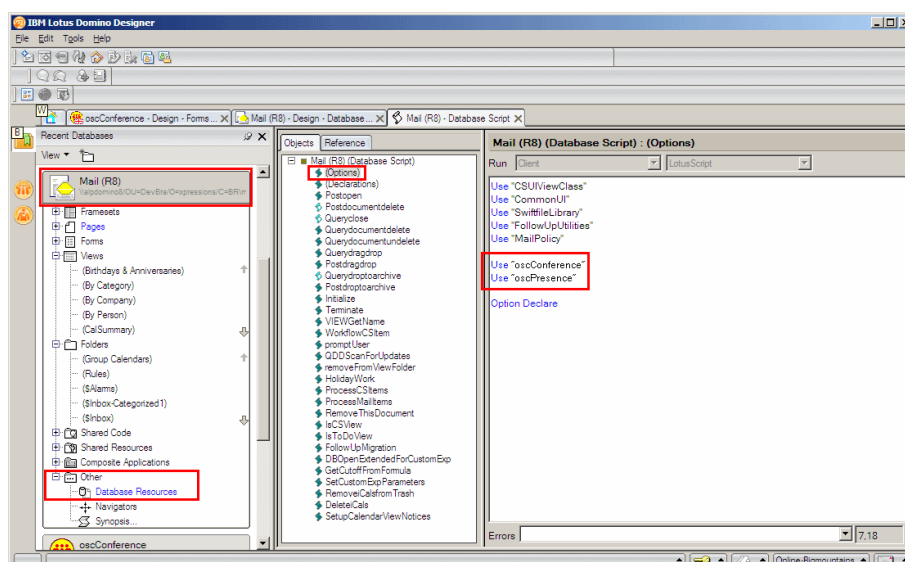
4.14.12.8 Configuring the Activation of the Presence Plugin Thread

The presence plugin thread must become active as soon as the mail application is opened in the IBM Lotus Notes client. To this, perform the following steps:

- 1) Open in the mail template database **Other > Database Resources > Database Script**.



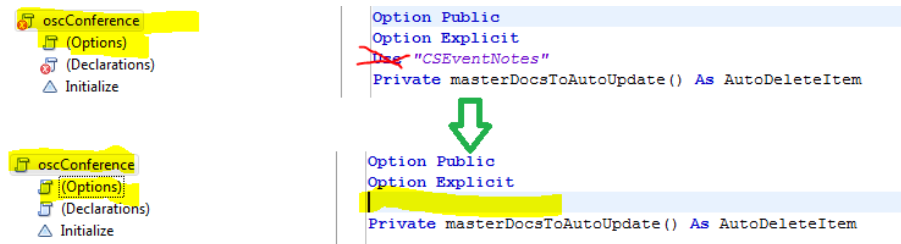
- 2) Click on the tab **Objects**.
- 3) Select **Mail (R8) (Database Script) > (Options)**.
- 4) Code is displayed in the **Mail (R8) (Database Script) : (Options)** section.
- 5) Look for the following code line in this code:
Option Declare
- 6) Paste the following line before this code line:
Use "oscConference"
Use "oscPresence"



4.14.12.9 Additional Adaptation of the templates for Notes

In order to configure the template the following steps are necessary:

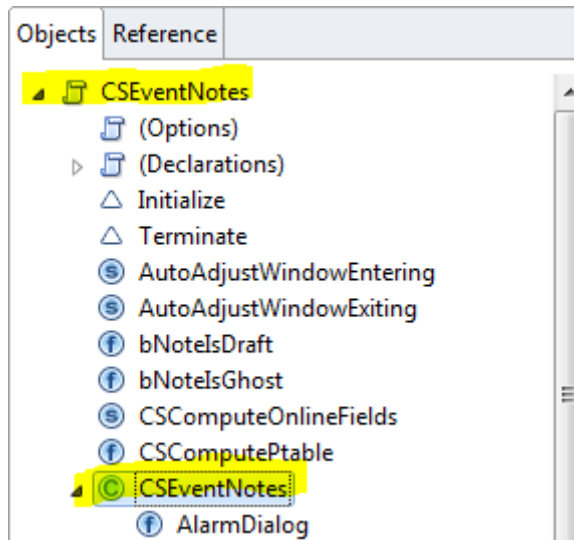
- 1) Remove the reference to "CSEventNotes" from oscConference. That includes also language variants.



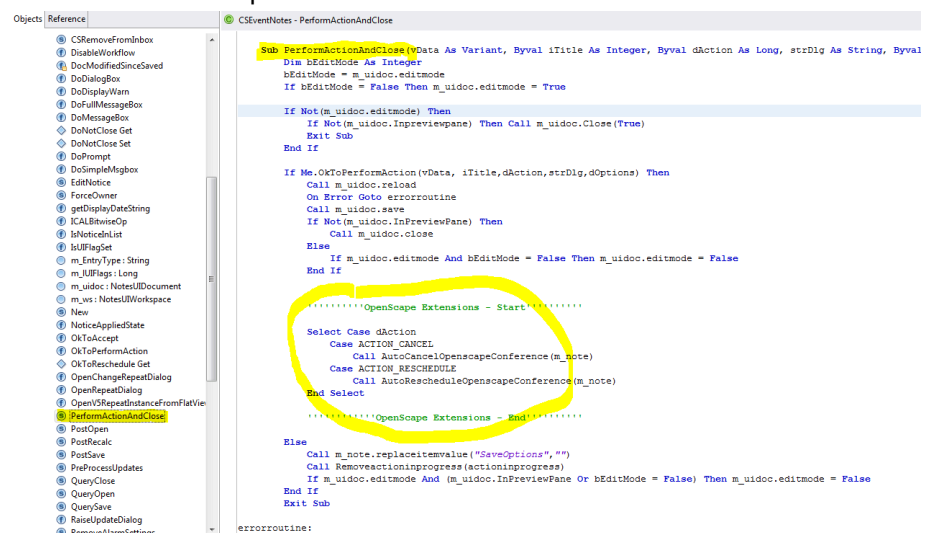
- 2) Add a reference to "oscConference" at "CSEventNotes"



- 3) Locate the definition of class “CSEventNotes” and there inside the function “PerformActionAndClose”.



Add the code in the picture



The text is:

```

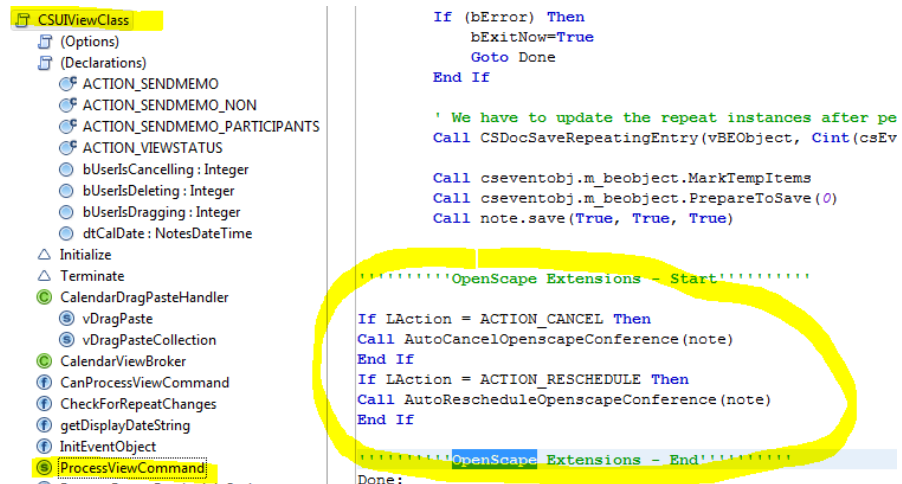
'//////// OpenScope Extensions - Start '////////
Select Case dAction
    Case ACTION_CANCEL
        Call AutoCancelOpenscapeConference(m_note)

    Case ACTION_RESCHEDULE
        Call
        AutoRescheduleOpenscapeConference(m_note)
End Select
'//////// OpenScope Extensions - End '////////

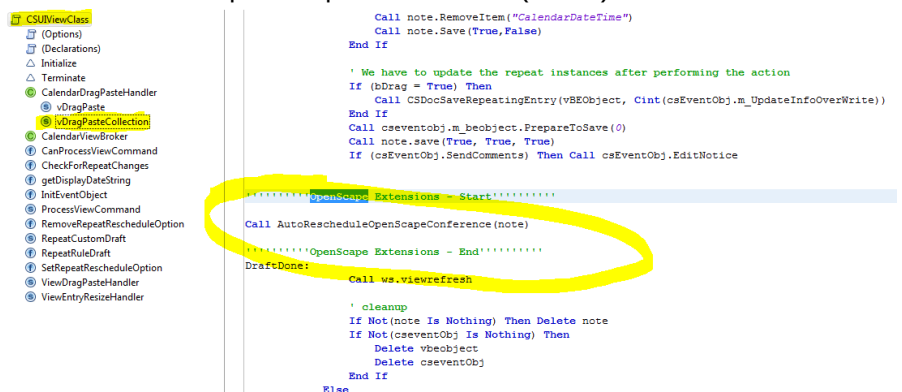
```

- 4) Recompile everything and check if it works. In some cases the Reschedule action is not covered which is normally in the templates. Double check the following steps.

- 5) Check inside “CSUIViewClass” under “ProcessViewCommand” if the marked code is there. If not, add it.



- 6) Check inside “CSUIViewClass” under “vDragPasteCollection” if the marked code is there. If not add it. The marked code is: Call AutoRescheduleOpenScapeConference(note)



Recompile and check again.

4.14.12.10 Configuring the Deletion of Conferences

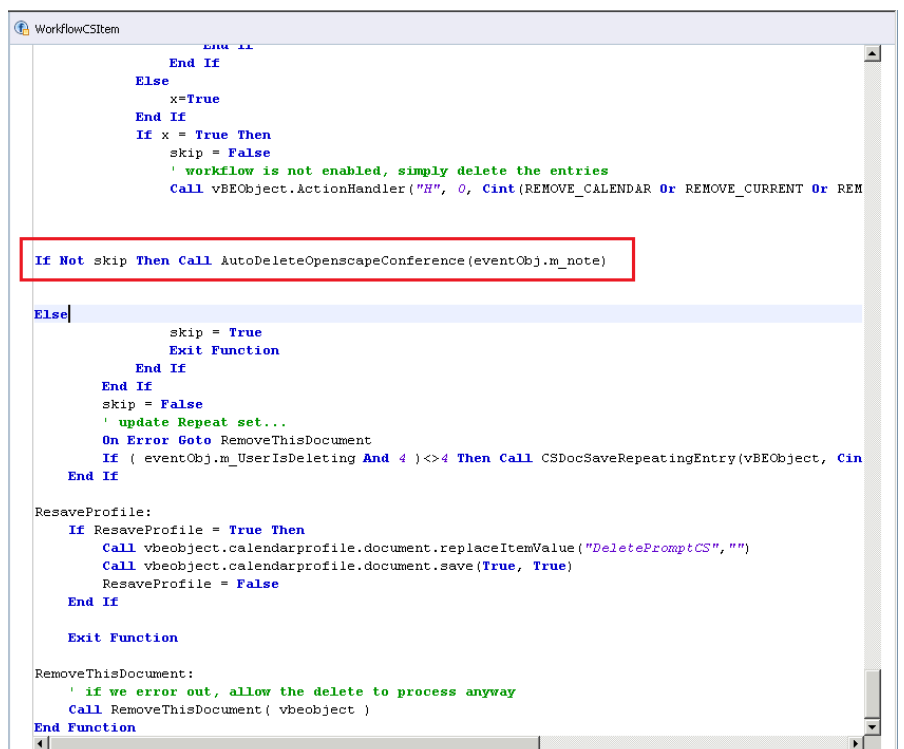
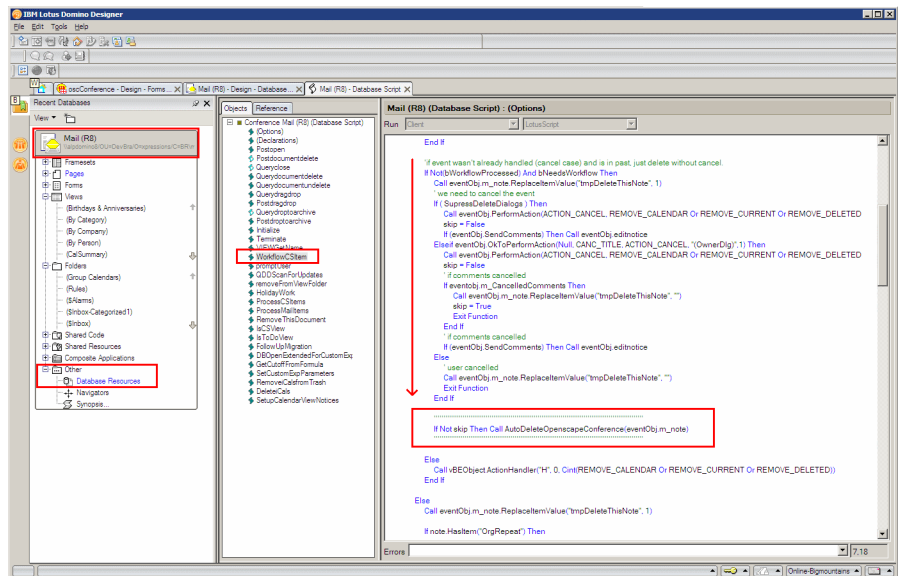
To enable users deleting UC Application conferences via their IBM Lotus Notes calendar, three function calls must be added in the database script. Furthermore, the script library **CSUIViewClass** must be expanded.

Start the configuration

How to adjust the database script and the script library:

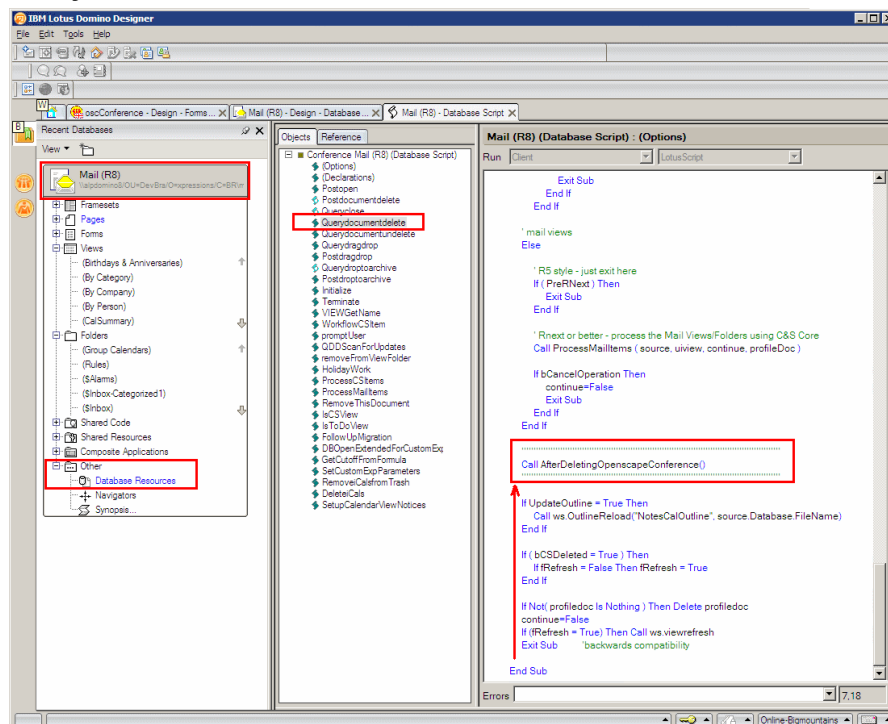
- 1) Select **Mail (R8) (Database Script) > WorkflowCSItem**.

- 2) Code is displayed in the **Mail (R8) (Database Script) : WorkflowCSItem** section. There are two positions to locate, so scrolling maybe needed.

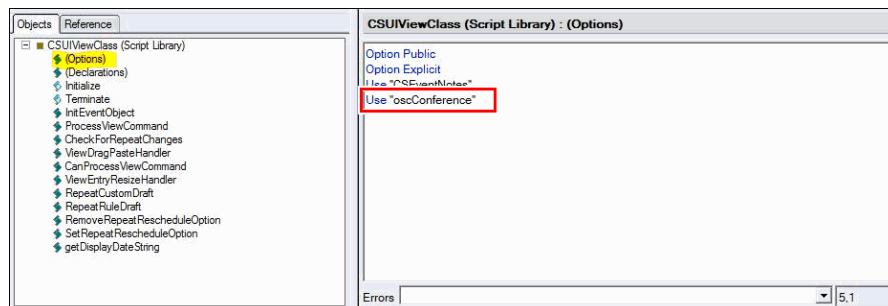


- 3) Insert the following line in the two indicated positions:
- If Not skip Then Call
AutoDeleteOpenscapeConference(eventObj.m_note)
- 4) Select **Mail (R8) (Database Script) > QueryDocumentDelete**.

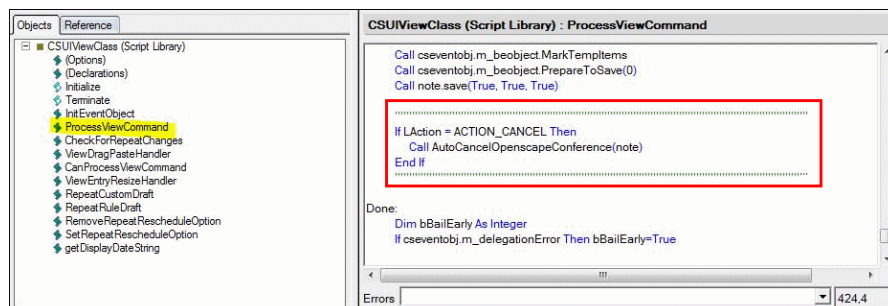
- 5) Code is displayed in the **Mail (R8) (Database Script) : QueryDocumentDelete** section.



- 6) Insert the following line in the bottom section in the indicated position:
Call AfterDeletingOpenScapeConference()
- 7) Search the mail template database for the script library **CSUIViewClass**.
- 8) Code is displayed in the **CSUIViewClass (Script Library) : Options** section.



- 9) Insert the following line at the bottom of this code:
Use "oscConference"
- 10) Code is displayed in the **CSUIViewClass (Script Library) : ProcessViewCommand** section.



- 11) Insert the following lines in the indicated position:

```

.....
If LAction = ACTION_CANCEL Then
Call AutoCancelOpenscapeConference(note)
End If
.....

```

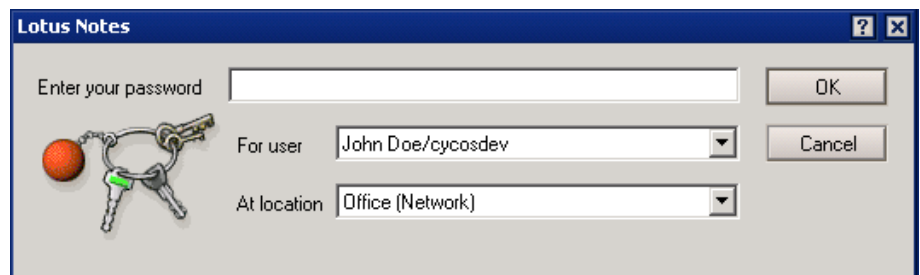
- 12) Recompile all scripts in the mail template database. Save the database resource and close the IBM Lotus Domino Designer.

You have now performed all necessary modifications in the mail template database.

4.14.12.11 Activating the Configuration for IBM Lotus Notes Users

Transfer the modifications in the mail template database to the mail databases of all IBM Lotus Notes users and install the .NET-Assemblies by performing the following steps:

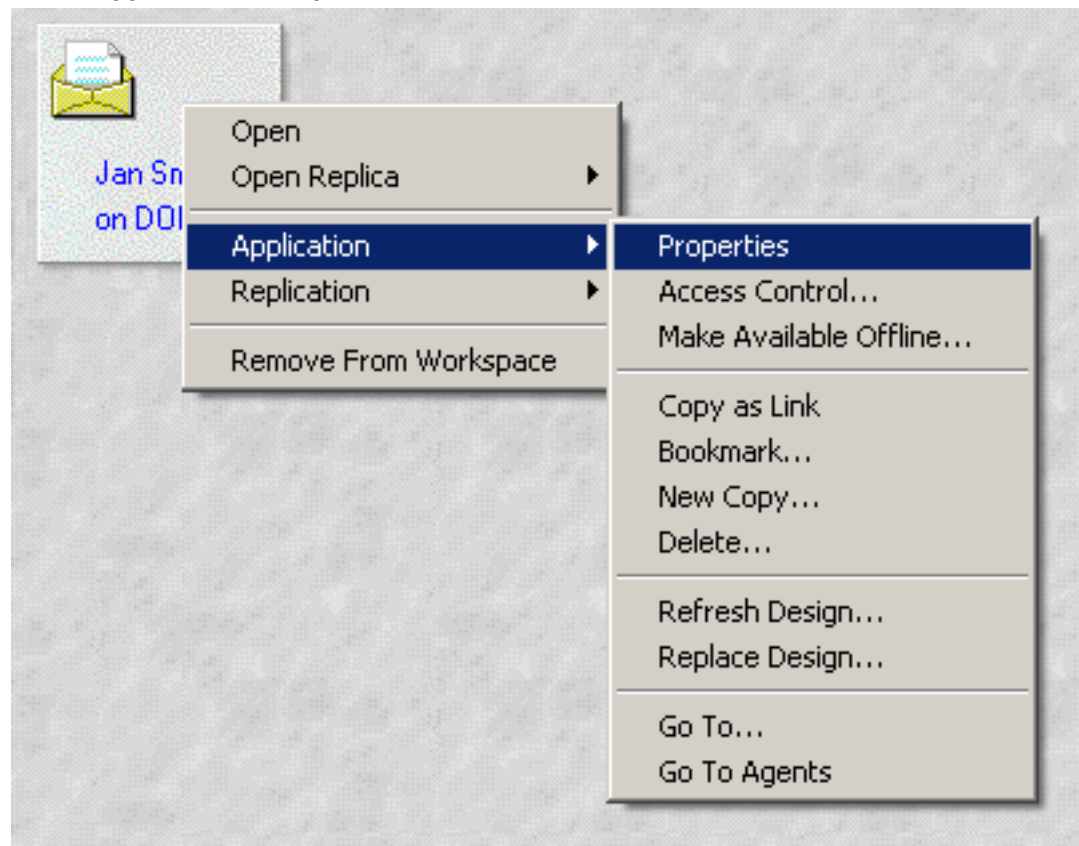
- 1) Open an IBM Lotus Notes client from which you can access the mailbox of an IBM Lotus Notes user as administrator.



Enter the password and click on **OK**.

- 2) Using the right mousebutton, select in the workspace the mail database of the IBM Lotus Notes user who is to deploy the plugin.

3) Select **Application > Properties**.



The property window of the database opens.

- 4) Click on the fourth tab.

The screenshot shows a 'Database' configuration window with a blue title bar and a toolbar. The 'Design is not hidden' status is shown at the top. The 'Options' section includes checkboxes for 'Allow design locking', 'List in Database Catalog' (checked), 'Show in 'Open Database' dialog' (checked), 'Include in multi-database indexing', 'Do not mark modified documents as unread' (checked), and 'Mark parent note on reply or forward' (checked). The 'Inheritance' section is highlighted with a red box, showing the 'Inherit design from master template' checkbox checked and the 'Template name' field containing 'StdR8Mail'. Below this, the 'Template version is 8.0 (31/07/2007)' is displayed. Other options in the 'Inheritance' section include 'Refresh design on admin server only', 'Database file is a master template', and a 'Template name' field. The 'Multilingual Options' section at the bottom includes checkboxes for 'Multilingual database', 'Unicode standard sorting', and dropdown menus for 'Default language', 'Default region', and 'Default sort order'.

- 5) Verify that the **Inherit design from master template** checkbox is ticked off and that the template name of the previously changed mail template database is present in the **Template name** field.

IMPORTANT: Do not confuse the template name of the mail template database with the file name or title of this database. The file name of the mail template database is typically mail8.ntf, the title is Mail (R8) and the template name

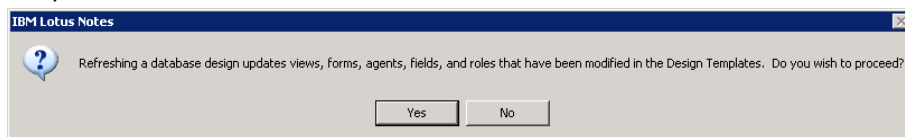
StdR8Mail. You find all three values in the properties window of the mail template database.

- 6) If the **Inherit design from master template** checkbox was already ticked off in the previous step you need to select the user's mail database with the right mousebutton in the workspace and choose one of the following menu options:

- German: **Datenbank > Gestaltung aktualisieren ...**
- English: **Database > Replace design ...**
- French: **Base de documents > Actualiser conception ...**
- Italian: **Database > Aggiorna impostazione ...**
- Spanish: **Base de dados > Actualizar disenio ...**



- 7) Select the IBM Lotus Domino server on which the previously changed mail template database is found and click the **OK** button.



- 8) Click the **Yes** button.
9) Execute steps 1 to 8 for all other IBM Lotus Notes users.

You have thus configured the Lotus IBM Domino server for OpenScape - Conference Extension for Lotus Notes.

4.15 Configuring the LDAP Directory Connection

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

NOTICE: Special requirements must have been met for configuring the LDAP connection. See [Configuration requirements for the LDAP connection](#) on page 85.

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

Via the LDAP connection the OpenScope system can also be connected to an Active Directory. Such a connection does not allow access to global contact lists in MS Exchange, though.

How to configure the connection of an LDAP directory:

- 1) [Configuring the Connection to the LDAP Directory](#)
- 2) Configuring the Field Assignment (Mapping) "
- 3) [Restarting the LDAP Connector Service](#)
- 4) [Configuring the LDAP User Access](#)
- 5) **If a Facade server is used:**
[Rebooting the Facade Server](#)

These steps are described in detail in the following sections.

4.15.1 Configuring the Connection to the LDAP Directory

So that the LDAP connector can access the LDAP directory, you need to configure the LDAP directory connection data in the LDAP connector.

To check if your Windows server supports LDAPS and has the required certificates for this purpose on the BE node execute:

```
openssl s_client -connect LDAPS.SERVER.FQDN:636 -showcerts
```

For UM LDAPS connection (UM sync with LDAP):

You can enable the Use Secure Connection in the LDAP Connection window and then click the Retrieve Certificate button to view and accept the certificate.

For UC LDAPS connection (UC contact service queries against LDAP, contact search, number to name resolution etc):

NOTICE: Name resolution does not work properly for an LDAP contact when the phone number has spaces in it. Phone Numbers in Active Directory should be stored without spaces. If phone numbers in Active Directory contain spaces only exact matching search can be performed successfully from UC.

Use port 636 and useSSL=true in the LDAP connection under CMP UC settings.

Then navigate to the Windows server > Certificates and get the cer file for this machine, e.g. save with name ldapserver.cer.

You should now import it in the default Java keystore on the BE node. Choose an alias e.g. ldapserver

Execute:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -import -keystore /opt/siemens/share/ibm-java-x86_64-80/jre/lib/security/cacerts -storepass changeit -alias ldapserver -import -file ldapserver.cer
```

Restart symphonia.

Start the configuration

How to configure the connecting data in the LDAP connector:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > LDAP**.
A list of all LDAP connections configured in the OpenScape UC Application is displayed.
- 3) Tick off the checkbox of the LDAP connection you want to configure and click on **Edit**.
The dialog with the settings of the LDAP connector opens.
- 4) Specify under the **connection.displayName** connection property the name under which the LDAP directory is to be displayed in the OpenScape clients.
- 5) Specify the following data under the **connection.serverURL** connection property:
 - IP address under which the LDAP directory server can be reached.

NOTICE: If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

- Port via which the LDAP connector is to exchange data with the LDAP directory server.

Separate IP address and port by a colon.

Example: 10.10.10.10:389

NOTICE: In a Windows 2003 Active Directory domain with several domain controllers the LDAPconnector must be configured to communicate with the global catalog server. For unencrypted communication, port 3268 must be configured, or port 3269 for SSL-encrypted communication.

- 6) If the LDAP connector is not to access the LDAP directory anonymously, proceed as follows.
 - a) Specify the user account with which the LDAP connector is to access the LDAP directory under the **connection.username** connection property.

NOTICE: In case of a connected Active Directory for Windows 2003 Server, deploying a default domain user is sufficient. The user need not have administrative privileges.

- b) Specify the password for the user account used under the **connection.password** connection property.

- 7) Specify under the **connection.useSSL** connection property whether the communication between LDAP connector and LDAP directory is to be encrypted via SSL.
- If the communication is to be encrypted via SSL, enter **true** in the field of this property.

You find continuative information about configuring security certificates in [Configuring a Certificate Strategy](#) on page 646.

NOTICE: If you want to use SSL, you need to specify the port for SSL under the **connection.serverURL** property.

- If the communication is not to be encrypted via SSL, enter **false** in the field of this property.
- 8) Specify the search base with which the LDAP connector is to access the LDAP directory under the **searchBase** connection property.

NOTICE: A search base must always be a subdirectory.

- 9) Specify under the **SearchMask** connection property the search mask the LDAP connector is to use for each search request.

The search mask must contain the expression **#s** at least once. The LDAP connector replaces this expression with the search filter in case of a search request.

Example: (&#s(objectclass=dingo)(status=OK)(!(multiple-link=*)))

- 10) Under the **maxRecords** connection property, specify the maximum number of data records the LDAP directory is to deliver upon a search request.

If an appropriate limit has already been configured in the LDAP directory, the **maxRecords** setting is noneffective.

- 11) Specify under the **useDNasID** connection property if the distinguished name of an LDAP entry is to be used as unique ID in case of a directory search.

This property must be set to **true** if the connected LDAP directory does not have a field with unique data ID.

- 12) Specify under the **connection.followReferrals** connection property whether LDAP directory references are to be pursued.

- If the LDAP directory references are to be pursued, enter **true** in this property's field.
- If the LDAP directory references are not to be pursued, enter **false** in this property's field.

You have now configured the LDAP directory connection data in the LDAP connector.

4.15.2 UC LDAPs connection configuration

Import the signed certification chain of the LDAP certificate in the java truststore cacerts and change the LDAP connector configuration to SSL.

Make sure that the addressed LDAP server in the connector configuration matches with the issued to or SAN.

Start the configuration

- 1) You must get the customer certificate using the following command:
 - a) `openssl s_client -connect <LDAP directory Server IP address>:636`
 - b) Copy the certificate part from:
`-BEGIN CERTIFICATE`
to:
`-END CERTIFICATE`
for example like the following:
`openssl s_client -connect dc.gcsstg.net:636 2>/dev/null </dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > LDAPServerCert.pem`
 - c) Paste in new file (created with vi as example)
- 2) Name this file with .pem extension, for example: LDAPcert.pem
- 3) Import it in the following keystore file:
 - a) For a Simplex:
`/enterprise/share/ibm-java-i386-71/jre/bin/keytool -import -file LDAPcert.pem -alias openscapeucldaps -keystore /enterprise/share/ibm-java-i386-60/jre/lib/security/cacerts -storepass changeit`
 - b) For a Small or Large:
`/opt/siemens/share/ibm-java-i386-71/jre/bin/keytool -import -file LDAPcert.pem -alias openscapeucldaps -keystore /opt/siemens/share/ibm-java-i386-60/jre/lib/security/cacerts -storepass changeit`
- 4) Restart the symphonia daemon: `/etc/init.d/symphoniad restart`
- 5) The second step is to activate the option "Use SSL" in the LDAP-Configuration. Eventually you need to customize the Port.
The Standard LDAP SSI Port is 636

NOTICE: Check that LDAPS port (default: 636) is open in the customer firewall.

4.15.3 Restarting the LDAP Connector Service

So that the settings performed for the LDAP connector service can take effect you need to restart the LDAP connector.

Start the configuration

How to restart the LDAP connector service:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.
A list of all system nodes and external links available in the entire system is displayed in the workspace.
- 3) Click the name of the system node on which OpenScape UC Application is installed.
A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Look in the list for the **LDAP Connector Service** component and select the associated checkbox.

IMPORTANT: By the following step, the LDAP connector service will be stopped and immediately restarted again without any further query. That interrupts the LDAP services of the OpenScape system.

- If the LDAP connector service has already been started, click on **Restart**.
The LDAP connector service stops and restarts again.
- If the LDAP connector service has been stopped, click on **Start / Stop**.
The LDAP connector service starts.

The new settings for the LDAP connector service will then take effect.

4.15.4 Configuring the LDAP User Access

To enable OpenScape users deploying the connected LDAP directory as global contact list, you need to configure the global contact lists of OpenScape UC Application accordingly.

Start the configuration

How to configure the user access to the LDAP directory:

- 1) Select in the **Domain** drop-down list of the CMP toolbar the domain in which you want to create the user account.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click **Accounts > Contact Settings > Global List**.

A list of all global contact lists available in the OpenScape system is displayed in the workspace.

- 4) Select the checkbox of the **LDAP Connector Service** contact list.
- 5) Click on **Save current selection**.

The Facade server must be rebooted (as described in the next section) for the changed contact list setting to take effect for Mobile client users.

4.15.5 Rebooting the Facade Server

NOTICE: You need to execute the configuration steps of this chapter only if you use one Facade server.

The optional Facade server caches the directory configured as global or private contact list in its local cache. This cache is not automatically updated if another directory is configured as private or global contact list. Therefore, you need to manually reboot the optional Facade server for another contact list to take effect.

Start the configuration

How to reboot the Facade server:

- 1) Open a shell on the computer system of the Facade server.

IMPORTANT: The following step terminates all Facade server services. If Mobile clients are connected to OpenScape UC Application at this time, the relevant connections are closed without any further prompt or waiting period.

- 2) Execute the following command:

```
/etc/init.d/facaded restart
```

The changed contact list is thus integrated in the local cache of the Facade server and users of a Mobile client may access the LDAP directory also.

The LDAP directory is now connected to OpenScape UC Application.

4.16 Configuring the Instant-Messaging Connection

IMPORTANT: Execute all configuration steps of this section that apply to Very Large Deployment for Very Large Deployment for every cluster.

NOTICE: An Openfire server and Microsoft Lync cannot both be connected to OpenScape UC Application.

NOTICE: Special requirements must have been met for configuring the instant-messaging connection. See [Configuration requirements for Instant Messaging Connection](#) on page 86.

NOTICE: If you want to deactivate the instant-messaging connection at a later date, you need to configure

IM_ENABLED=N0 in the following file: <Osc-Install¹¹>/HiPathCA/config/deployment.props

NOTICE: Some of the following configuration steps only need to be executed under certain conditions. If these conditions apply to a configuration step, they are highlighted in bold above the respective configuration step and indicated specifically for the step. A note at the beginning of the respective chapter also indicates the restricted execution and the conditions applied.

How to configure instant messaging:

- 1) **For all deployment scenarios except Very Large Deployment with several Openfire servers:**

[Configuring the Openfire Server](#)

NOTICE: For Very Large Deployment with several Openfire servers you configure the Openfire servers used in [Configuring the System Networking](#) on page 298.

- 2) **For Integrated Deployment:**

[Creating Packet Filter Rules in OpenScape Voice](#)

- 3) [Configuring the IM Address for OpenScape Users](#)
- 4) [Activating IM Communication Archiving](#)
- 5) [Creating and synchronizing Openfire User Accounts](#)

These steps are described in detail in the following sections.

4.16.1 Configuring the Openfire Server

NOTICE: You need **not** execute the configuration steps of this chapter if you use the deployment scenario Very Large Deployment with several Openfire servers. You configure these Openfire servers in [Configuring the System Networking](#) on page 298.

You configure the Openfire server via the web-based Openfire administration interface. You can start this administration interface in the CMP via the configuration dialog for presence and instant messaging.

Start the configuration

How to configure the Openfire server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Presence & IM**.

The configuration dialog for presence and instant messaging opens.

¹¹ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

3) Select **Start Openfire Admin-UI**.

The login dialog for the administration interface of the Openfire server opens.

NOTICE: The **Start Admin UI** button is only active if the connection data for the Openfire server was configured and tested. This should have been done during the OpenScape UC Application setup.

4) Log on to the Openfire server under an administrator account.

In doing so please heed the following:

- After a new installation of the Openfire server, the following default password is valid for the user accounts **administrator** and **admin**: **Asd123!**.
- After an upgrade, the following default passwords are valid:
 - For the user account **administrator**, the default password is: **8ABWnmppzEOuxu1q**
 - For the user account **admin**, the default password is: **01*Test!**

NOTICE: The valid passwords can be changed individually on the Openfire administration interface. You find details about this in the Openfire server product documentation.

The Openfire administration interface opens.

- 5) Switch to the **Server > Server Settings** tab and select the **HTTP Binding** menu option.
- 6) Activate the option **Disabled – Clients will not be able to connect with this server using HTTP bindings**.

NOTICE: OpenScape UC Application connects to the Openfire server via the XMPP protocol only.

- 7) Select the **Registration & Login** menu option.
- 8) Activate under **Inband Account Registration** the option **Disabled – Users can not automatically create new accounts**.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 9) Activate under **Change Password** the option **Disabled – Users are not allowed to change their password**.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 10) Activate under **Anonymous Login** the option **Disabled – Only registered users may login**.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 11) Select the **Offline Messages** menu option.
- 12) Activate under **Offline Message Policy** one of the following options:
- **Bounce – Never store offline messages and bounce messages back to the sender.**
 - **Drop – Never store offline messages and drop messages so the sender is not notified.**

NOTICE: OpenScape clients dismiss messages about message deletion (bounce messages). The behavior of the OpenScape clients is thus the same for both options.

- 13) Select the **Private Data Storage** menu option.
- 14) Activate under **Set Private Data Policy** the option **Disabled Private Data Storage – Do not allow server-side storage**.

NOTICE: This feature is not supported by OpenScape clients.

- 15) Select the **File Transfer Settings** menu option.
- 16) Activate under **Proxy Service** the option **Disabled – This server will not act as a file transfer proxy**.

NOTICE: This feature is not supported by OpenScape clients.

- 17) Select the **Search Service Properties** menu option.
- 18) Activate under **Service Enabled** the option **Disabled – Clients will not be able to search for users**.

NOTICE: This feature is not supported by OpenScape clients.

You have thus configured all settings of the Openfire server that are required for connecting OpenScape UC Application. Please obtain information about further Openfire server settings from the Openfire server documentation.

4.16.2 Creating Packet Filter Rules in OpenScape Voice

NOTICE: You need to execute the configuration steps of this chapter for Integrated Deployment only.

The web server component uses the ports 5262, 4710 and 4711 for the instant-messaging communication. These ports are blocked by the firewall of

OpenScape Voice. To open it you need to create two new packet filter rules in OpenScape Voice. In this process you can assign any names to the packet filter rules.

Start the configuration

How to create the new packet filter rules in OpenScape Voice:

- 1) Start as user **srx** startCli of OpenScape Voice.
- 2) Log on as **sysad**.
- 3) Select 6 (Application Level Management).
- 4) Select 8 (Network Element Security Management).
- 5) Select 4 (Packet Filter Rules Security Management).
- 6) Select 1 (Create).
- 7) Enter the following settings for the new packet filter rule:

Remote IP Address:	<IP address of the IM server>
Transport Protocol:	3 (TCP)
Remote Port Begin:	5262
Direction:	3 (incoming + outgoing)
Local Port Begin:	0 (all ports)
Action:	1 (Allow)

- 8) Adopt the new packet filter rule.
- 9) Select 1 (Create).
- 10) Enter the following settings for the second new packet filter rule:

Remote IP Address:	<IP address of the IM server>
Transport Protocol:	3 (TCP)
Remote Port Begin:	0 (all ports)
Direction:	1 (incoming)
Local Port Begin:	4710 (used via js-soc)
Local Port End:	4711 (used via js-soc-ssl)
Action:	1 (Allow)

- 11) Adopt the new packet filter rule.
- 12) Select 4 (display) to check the settings of the configured packet filter rule once more.

The ports required for the instant-messaging communication of the WebClient component are now open for Integrated Deployment.

4.16.3 Configuring the IM Address for OpenScape Users

The Instant Messaging address of an OpenScape user is configured in the contact data of the relevant user profile.

You can assign the Instant Messaging address to users either manually or by bulk import. How to use bulk import is described in the *OpenScape Common Management Platform, Administrator Documentation* manual.

Start the configuration

How to assign a user an Instant Messaging address manually:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain in which the desired user has been created.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 3) In the navigation tree, click on **Accounts > List**.

A list of all users configured in the selected domain appears in the workspace.

- 4) Click on the login name of the desired user.

The dialog with the settings of the relevant user opens.

- 5) Switch to the **Contact Information** tab.

- 6) Specify the desired Instant Messaging address of the user in the **IM Address** field – *Example:* Monica.Sample@domain.

NOTICE: The Instant Messaging address of a user is composed of the respective OpenScape user name (**Username**) and the domain name specified upon the setup of the relevant Openfire server. *Example:* Monica.Sample@openfire.mycompany.com

- 7) Click on **Save** to copy the setting.

You have now manually assigned an Instant Messaging address to the user.

4.16.4 Activating IM Communication Archiving

You can activate archiving the instant messaging communication in the Openfire server to search the communication data collected in this way by individual criteria later.

Start the configuration

How to activate archiving the instant messaging communication:

- 1) Log on to the Openfire server under an administrator account.

In doing so please note:

- After a new installation of the Openfire server, the following default password is valid for the user accounts **administrator** and **admin**: **Asd123!**.
- After an upgrade, the following default passwords are valid:
 - For the user account **administrator**, the default password is: **8ABWnmppzEOuxu1q**
 - For the user account **admin**, the default password is: **01*Test!**

NOTICE: The valid passwords can be changed individually on the Openfire administration interface. You find details about this in the Openfire server product documentation.

The Openfire administration interface opens.

- 2) Switch to the **Server > Archiving** tab and select the **Archiving Settings** menu option.
- 3) Activate the **Conversation State Archiving** option to archive the general statuses of the instant messaging connections.
- 4) Activate under **Messaging Archiving** the options desired for archiving the instant messaging message texts.
- 5) Select **Update Settings** to copy the changed settings.

The Openfire system creates now automatically an index for the archived data of the instant messaging connections. This process may take up to 15 minutes.

Subsequently, creating a new index will be triggered automatically every 15 minutes.

Details about how to search archived data are provided in [Searching archived Connection Data](#) on page 508.

The Openfire server is now connected to OpenScape UC Application.

4.16.5 Creating and synchronizing Openfire User Accounts

So that the OpenScape users can deploy the instant-messaging features of the Openfire server, a user account must be created on the Openfire server for each OpenScape user. The user accounts are created automatically and the later synchronization with OpenScape UC Application occurs automatically, too. OpenScape UC Application uses the Openfire Authentication Plugin and the Authentication Provider of OpenScape UC Application for this purpose.

An Openfire user account is created as soon as a user logs on to the Openfire server via OpenScape UC Application for the first time.

Manual creation or management of Openfire user accounts is thus not necessary.

NOTICE: The access passwords for OpenScape users are exclusively administered under OpenScape UC Application. Passwords on the Openfire server are not considered. If an

OpenScape user deploys an IM client alien to the system and changes his/her access password, only the password stored on the Openfire server changes. Consequently, there are two different passwords: The password under OpenScape UC Application and the one in the Openfire server. These two are not automatically synchronized. In this case the user needs to log on to OpenScape clients with the first password and to IM clients alien to the system with the second.

4.16.6 Disabling IM Communication Archiving

If you use an External Openfire server (with MySQL database) as Presence Provider and for some reason you need to disable Chat History you should perform the following:

- 1) Log on to the Openfire server under an administrator account.
- 2) Switch to the Server > Archiving tab and select the Archiving Settings menu option.
- 3) Deactivate the Conversation State Archiving option to archive the general statuses of the instant messaging connections.
- 4) Deactivate under Messaging Archiving the two options for archiving the instant messaging message texts.
- 5) Press the Update Settings button to save the settings.
- 6) Restart Openfire in order to make the changes visible to OpenScape UC.

4.16.7 Delete Chat Message

- It is possible to delete the messages and attachments the user have already sent.
- Delete chat message functionality is supported if chat history is enabled.
- It is possible to retain internally the deleted messages even if they have been removed and therefore not visible any longer to the user. This is achieved with the `conversation.keepOnDeletion` Openfire property that indicates whether the archiving of deleted messages is enabled or not. The default value of this property is set to false, meaning that all messages will be immediately deleted as soon as a delete request is received.
- All the messages/attachments that are temporarily archived after their deletion (`conversation.keepOnDeletion` is set to true) will still be deleted according to the value defined in the property Max Message Age of the Openfire Archive Settings.

4.17 Configuring the Connection to OpenScape Xpressions

IMPORTANT: In case of Very Large Deployment you need to execute the configuration steps described here for each cluster.

IMPORTANT: You can connect several OpenScape Xpressions systems to several UC Application systems with any assignment ($m \times n$ connection). You find details of the configuration concept

for such a connection in the *OpenScape UC Application, Planning Guide* manual. Executing the following configuration steps for an $m \times n$ connection correctly requires reading and understanding this concept description before the configuration.

NOTICE: Special requirements must have been met for configuring the OpenScape Xpressions connection. See [Configuration requirements for the OpenScape Xpressions connection](#) on page 86.

How to configure OpenScape Xpressions as voicemail system for UC Application users:

- 1) If required [Planning Details for an \$m \times n\$ Connection](#)
- 2) [Configuring Voicemail Numbers for Users](#)
- 3) [Assigning the Access Privilege](#)
- 4) [Displaying PhoneMail Settings](#)
- 5) [Configuring XPR PhoneMail](#)
- 6) [Configuring the Voice Portal Access](#)
- 7) [Installing the XPR Import Script](#)
- 8) [Configuring the XPR Import Script](#)
- 9) [Creating an XPR Import File](#)
- 10) [Importing an XPR Import File](#)
- 11) [Rebooting the XPR Server](#)
- 12) [Assigning a Privilege to XPR Users](#)
- 13) [Configuring the Web APL of OpenScape Xpressions](#)
- 14) [Configuring PhoneMail Script Settings](#)
- 15) [Creating a UC Application Import File](#)
- 16) [Importing a UC Application Import File](#)
- 17) [Configuring OpenScape Web Client](#)
- 18) [Changing UC Application User Profiles](#)

These steps are described in detail in the following sections.

You find continuative information about the technical design of the OpenScape Xpressions connection in [OpenScape Xpressions Connection](#) on page 36.

4.17.1 Planning Details for an $m \times n$ Connection

You can connect several OpenScape Xpressions systems to several UC Application systems with any assignment ($m \times n$ connection).

Before you can configure such an environment with the steps to be executed in the following chapters, you must perform some preparative planning. To do this, create a networking plan according to the architecture you desire. In doing so plan the following:

- The structure in which the OpenScape Xpressions and UC Application system shall be networked with each other.

- The system ID to be used in the OpenScape Xpressions systems for the various UC Application systems.

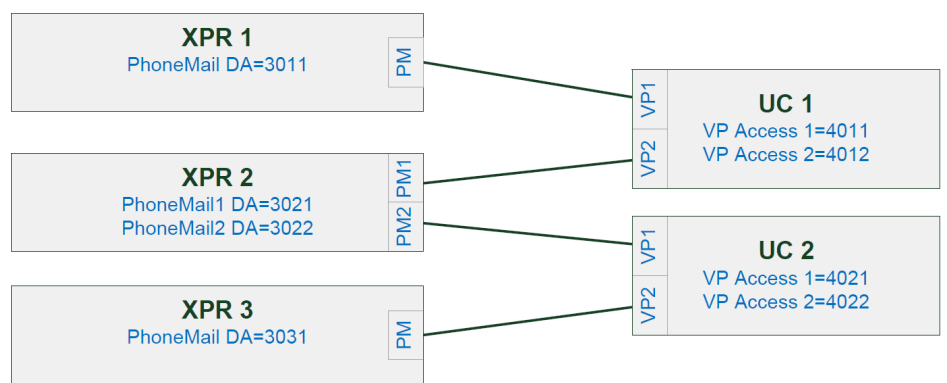
NOTICE: The system ID serves for differentiating the connections to different UC Application systems in an OpenScape Xpressions system. If only a single UC Application system shall be connected to an OpenScape Xpressions system, a system ID for the UC Application system need not necessarily be used in this OpenScape Xpressions system.

- The number and settings of required PhoneMail entities in the OpenScape Xpressions systems. Among these, the phone numbers for the Direct Access and the trusted-transfer settings.
- The number and settings of required voice portal accesses in the UC Application systems. Among these, the phone numbers for the voice portal access and the trusted-transfer settings.
- The distribution of the user accounts of the UC Application systems among the connected OpenScape Xpressions systems.

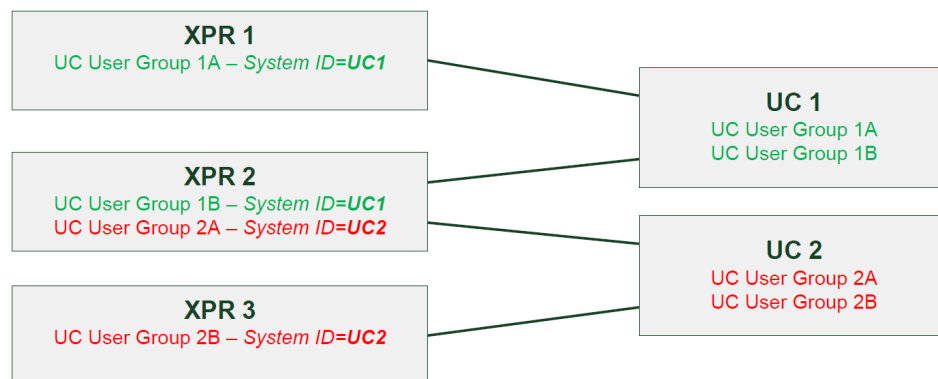
Examples: – Distribution according to the user accounts' initials –
Distribution according to company departments

Example:

PhoneMail entities & voice portal accesses



Networking structure & user account distribution



Distribution of User Accounts

UC User Group 1A	– UC User Accounts H – Z on System UC 1
UC User Group 1B	– UC User Accounts A – G on System UC 1
UC User Group 2A	– UC User Accounts A – G on System UC 2
UC User Group 2B	– UC User Accounts H – Z on System UC 2

4.17.2 Configuring Voicemail Numbers for Users

The UC Application system uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called UC Application users. In this way no call is lost even if the called UC Application user cannot accept the call.

In case of the OpenScape Xpressions connection the UC Application system uses the PhoneMail script of the XPR server as voicemail system. Consequently, you need to configure the phone number of the Guest/Forward Access of the PhoneMail script as voicemail number for UC Application users.

You can assign the number of your voicemail box to users either manually or by bulk import. How to use bulk import is described in the *OpenScape Common Management Platform, Administrator Documentation* manual.

NOTICE: If you do not assign a voicemail number to a user, he/she does not see the Voicemail tab on the OpenScape Web Client user interface. In order to change this behavior, you can configure the value **FALSE** for the **VoicemailNumberRequired** setting in the following configuration file: `<Osc-Install12>/HiPathCA/config/common/TelasWeb.cfg` If you do not assign a voicemail number to a user, calls will not be automatically forwarded to the user's voicebox.

Start the configuration

How to assign an UC Application user a voicemail number manually:

¹² `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain in which the desired user has been created.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) On the **Configuration** navigation tab of the CMP click on the **Unified Communications** navigation menu item.
- 3) In the navigation tree, click on **Accounts > List**.

A list of all users configured in the selected domain appears in the workspace.

- 4) Click on the login name of the desired user.

The dialog with the settings of the relevant user opens.

- 5) Switch to the **Resources** tab.

All resources assigned to the user are displayed.

- 6) Click on **Assign**.

A list of all phone numbers that can be assigned as voicemail number to the user appears.

If the list does not contain any phone numbers, you need to create a new phone number. Proceed as follows:

- a) Click the **Add** button.

The dialog for creating a new voicemail number opens.

- b) Enter in the **Number** field the voicemail number to which incoming calls may be routed for the relevant user.

In this case thus the phone number for the Guest / Forward Access of the PhoneMail script. In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems this is the PhoneMail script of the OpenScape Xpressions system the respective user is assigned to.

- c) Click **OK** to create the new phone number.

The newly created phone number is now displayed in the phone number list.

- 7) Select the check box of the voicemail number to which incoming calls are to be routed for the relevant user if required.

In this case thus the phone number for the Guest / Forward Access of the PhoneMail script. In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems this is the PhoneMail script of the OpenScape Xpressions system the respective user is assigned to.

- 8) Click on **OK** to copy the selected phone number for the user.

- 9) Click on **Save** to copy the settings.

- 10) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must execute the described steps on all UC Application systems.

You have now manually assigned the UC Application user a voicemail number.

4.17.3 Assigning the Access Privilege

So that an UC Application user can deploy OpenScape Xpressions as voicemail system, an UC Application user profile must have been assigned to him/her that contains the **Voicemail –Xpressions** access privilege.

You can proceed as follows:

- Create a new user profile that contains exclusively the access privilege **Voicemail Xpressions**. Then assign this user profile to all UC Application users who are to deploy OpenScape Xpressions as voicemail system in addition.
- Activate the access privilege **Voicemail Xpressions** in a non-standard user profile already assigned. All UC Application users who have already been assigned this user profile then deploy OpenScape Xpressions as voicemail system.

How to create a new UC Application user profile describes [Creating a User Profile](#) on page 109.

Start the configuration

How to activate the **Voice Mail – Xpressions** access privilege in an existing UC Application user profile:

NOTICE: The privileges of default profiles cannot be modified.

- 1) Select in the **Domain** combo box of the CMP toolbar the domain in which you want to change the user profile.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **CMP** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click on **General > Profiles**.

A list of all profiles configured in the selected domain appears in the workspace.

- 4) Click on the name of the profile for which you want to activate the **Voice Mail Xpressions** access privilege.

The dialog with the settings of the relevant profile opens.

- 5) Select the check box for the privilege **Essential > Voice Mail Access via ... > ...via Xpressions**.

NOTICE: The product names and licenses required for the activated rights are displayed in the **Licenses** area.

- 6) Click on **Save** to copy the settings.
- 7) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must execute the described steps on all UC Application systems.

You have now activated the **Voice Mail – Xpressions** access privilege in the UC Application user profile. All UC Application users who have been assigned this user profile can now use OpenScape Xpressions as voicemail system.

4.17.4 Displaying PhoneMail Settings

So that the XPR monitor displays the PhoneMail settings for the connection to OpenScape UC Application, you must extend the customer parameters for the PhoneMail script.

Start the configuration

How to have the settings for the connection to OpenScape UC Application displayed:

- 1) Open the XPR monitor and log on with an administrator account.
- 2) In the modules window of the XPR monitor select **<Settings> – IpApl – Set Options**.

The IP APL configuration dialog opens.

- 3) Switch to the **Protocols** tab.
- 4) Select the **Xpressions PhoneMail** protocol.
- 5) Select **Edit** .

The dialog for configuring the PhoneMail script opens.

- 6) Switch to the **Script** tab.
- 7) Select **Parameters**.

The dialog with the parameter settings of the PhoneMail script opens.

- 8) Switch to the **Customer** tab.
- 9) Supplement value **-ttm** in the **Parameters** field.
- 10) Select **OK** to save the new parameter.
- 11) Select **OK** to save the modifications in the script settings.
- 12) Select **OK** to save the script settings for the Telematic APL.
- 13) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

In the XPR monitor the parameter dialog of the PhoneMail script now contains the additional **OpenScape** tab, which you need in the next configuration step. This tab contains the settings for the OpenScape Xpressions connection.

4.17.5 Configuring XPR PhoneMail

You need to configure different settings in the PhoneMail script of the XPR server for the OpenScape Xpressions connection. These settings are required for the communication with OpenScape UC Application.

NOTICE: If an OpenScape Xpressions system is connected to several UC Application systems, an individual PhoneMail entity must be configured in the OpenScape Xpressions system for each of these connections.

Start the configuration

Configure the PhoneMail script of the XPR server for the OpenScape Xpressions connection by continuing in the XPR monitor as follows.

- 1) In the modules window of the XPR monitor select **<Settings> – IpApl – Set Options**.

The IP APL configuration dialog opens.

- 2) Switch to the **Protocols** tab.
- 3) Select the **Xpressions PhoneMail** protocol.
- 4) Select **Edit** .

The dialog for configuring the PhoneMail script opens.

- 5) Switch to the **Script** tab.
- 6) Select **Parameters**.

The dialog with the parameter settings of the PhoneMail script opens.

- 7) Switch to the **OpenScape** tab.
- 8) Activate the option **OpenScape Integration by Trusted Transfer Mode**.
- 9) In the **Remote Trusted-Domain call number** field specify the phone number under which the user access of the trusted-transfer mode can be reached in the voice portal.

You configured this phone number in [Configuring the Voice Portal Access](#) on page 281.

- 10) In the **Trusted Domain ID** field specify the domain ID that you use for the OpenScape Xpressions connection.

This specification must correspond to the value you configured for the voice portal under **Trusted Transfer Domain** (cf. [Configuring the Voice Portal Access](#) on page 281).

- 11) Enter the * character in the **Protocol Schema Start Character** field.
OpenScape UC Application uses the * character as fixed start character.
- 12) Enter number **13** in the **Caller number Maximum Length** field.
- 13) Specify in the **Voicebox number maximum length** field how many digits are used for the voicebox extensions.

This specification must correspond to the value you configured for the voice portal as **Account number** under **Xpressions Parameter Configuration** (cf. [Configuring the Voice Portal Access](#) on page 281).

- 14) Select **OK** to save the settings for the OpenScape Xpressions connection.
- 15) Select **OK** to save the modifications in the script settings.
- 16) Select **OK** to save the script setting for the IP APL.
- 17) If the OpenScape Xpressions system shall be connected to several UC Application systems: Configure an individual PhoneMail entity for each OpenScape Xpressions system to be connected and configure it as described.
- 18) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

You have now configured the PhoneMail script for the OpenScape Xpressions connection.

4.17.6 Configuring the Voice Portal Access

You must configure an individual voice portal access for the OpenScape Xpressions connection and perform various trusted-transfer settings for this access.

NOTICE: The access for the trusted-transfer mode does not provide direct voice portal access to users. It can only be used for the server-server communication between OpenScape Xpressions Server and UC Application Server.

Start the configuration

How to configure an individual access for the trusted-transfer mode:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the UC Application system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select the link of the **Voiceportal** application in the list.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the **Voiceportal** application.

6) Create a new application profile as follows.

- a) Select the radio button of the profile **start (Voice Portal access)** and select **Copy**.

The configuration dialog for a new application profile opens.

- b) Specify under **Profile name** a name for the new application profile – e. g. startTTM.

The application profile will be managed in the voice portal plug-in under this name.

NOTICE: You may enter only letters and numbers in the **Profile name** field.

- c) Switch to the **Operation Mode** tab.
- d) Enter in the **Xpressions Number** field the phone number that is configured for the **Direct Access** in the PhoneMail configuration of the XPR server to be connected.

You find the Direct Access setting in the XPR monitor under: **IP APL Settings > Protocols > Xpressions Phonemail > General > Direct Access**

NOTICE: If an OpenScape Xpressions system is connected to several UC Application systems, an individual PhoneMail entity must have been configured in the OpenScape Xpressions system for each of these connections. Be sure to use the Direct Access phone number of the correct PhoneMail entity.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications

system to the OpenScape Media Server during the connection setup.

- e) Enter in the **Trusted Transfer Domain** field a number that is used as domain number for the OpenScape Xpressions connection.

This number may comprise a maximum of two digits, as this length is defaulted by the XPR server.

You need to configure the same digit as domain number in the XPR server at a later date.

NOTICE: The domain number for the OpenScape Xpressions connection is in no way related to the domain management in the CMP.

- f) In the **Xpressions Parameter Configuration** section, specify value **13** under **ANI**.

NOTICE: The ANI is always handed over in the E.164 format.

- g) If required, use the **Account number** setting in the **Xpressions Parameter Configuration** section to adjust the calling number schema you wish to use for the OpenScape Xpressions connection.

Examples of calling number schemas with different extension lengths:

Extension length	Calling number schema UC Application system:
Three-digit	p0v1p1v1 p2v1 p3v13 p4v3 p5v2 p6v2
Four-digit	p0v1p1v1 p2v1 p3v13 p4v4 p5v2 p6v2
Five-digit	p0v1p1v1 p2v1 p3v13 p4v5 p5v2 p6v2

You find detailed information about the structure of the calling number schema in [Calling Number Schema](#) on page 37.

- h) Verify that value **2** is set for **Domain** under **Xpressions Parameter Configuration**.

This value is fixed by the XPR server.

- i) Check that value **2** is set for **Language** under **Xpressions Parameter Configuration**.

This value is fixed by the XPR server.

- j) Click on **Save** to copy the settings for the application profile.

- k) Click on **Close** to close the configuration dialog of the voice portal plug-in.

7) Execute the following steps to generate a terminal to which you assign the just created application profile:

a) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.

b) Select **Add**.

The configuration dialog for a new terminal opens.

c) Specify a unique identifier for the new terminal under **Terminal ID**.

Under this identifier the terminal is administered in the CMP.

d) Select the voice portal application profile you have just created under **Application**.

Depending on the voice portal application used it carries a name of the following format:

- Voiceportal#<application profile name >
- Voiceportalspeech#<application profile name >

e) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

f) Specify under **Address-expression** at least one phone number under which the guest access of the trusted-transfer mode shall be available.

Later, in the XPR PhoneMail configuration, this phone number will be referenced under **Remote Trusted-Domain call number**.

NOTICE: Calls for the defined phone numbers must be routed to the SIP trunk to the OpenScape Media Server by the communications system used. You need to configure the routing of the communications system accordingly.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

g) Determine under **Type** in which format the specified address expression is to be interpreted by the OpenScape Media Server.

h) Click on **OK** to copy the address settings.

i) If required, bind further addresses to the terminal in the described manner.

j) Click on **Save** to copy the settings for the terminal.

8) When you configure an $m \times n$ connection of OpenScape Xpressions and UC Application systems and the UC Application system is to communicate with several OpenScape Xpressions systems via Trusted Transfer Mode: Create an individual application profile and an individual terminal for each OpenScape Xpressions system to be connected.

Please heed the following for configuring the application profile:

- Specify in the **Xpressions Number** field the applicable phone number for the Direct Access of the XPR server to be connected.
- Specify in the **Trusted Transfer Domain** field the same number for all application profiles.

- In the **Xpressions Parameter Configuration** section, specify value **13** under **ANI** for all application profiles.
 - If required, use the **Account number** setting in the **Xpressions Parameter Configuration** section to adjust the calling number schema you wish to use for the respective XPR server to be connected.
- 9) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must execute the described steps on all UC Application systems.

You have now configured the communication settings for the OpenScape Xpressions connection in the voice portal.

4.17.7 Installing the XPR Import Script

So that the OpenScape Xpressions connection can operate smoothly, all UC Application user accounts must be imported in the XPR user database. In particular, the login data needs to be transferred to the XPR user database so that UC Application users can deploy their UC Application access data to log on to the XPR server.

The user accounts are automatically imported by an import script, which you need to install for the XPR server FI APL.

Start the configuration

How to install the FI APL import script:

- 1) Switch to the following directory.
 - In product versions before OpenScape Xpressions V7 on the product DVD of the XPR Server:

DVD1\AddOn\Openscape\FiSym
 - As of OpenScape Xpressions V7, on the computer system of the XPR Server:

<XPR Install>\AddOn\UCApplication\FiSym
- 2) Copy the FiSym.e file from this directory to the following directory of the installed XPR server:

<XPR Install>\res\FiApI

IMPORTANT: Check whether a current hotfix exists for the FiSym.e file. If so, copy it to the specified directory of the XPR server setup.

- 3) Create a new storage directory on the XPR server computer system.

Example: <XPR Install>\res\FiApI\OsUserImport

The FI APL shall later search this directory for files the content of which it can install in the user database of the XPR server.
- 4) Verify that the XPR server is privileged to read out of the newly created storage directory.
- 5) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

The XPR server import script is now installed.

4.17.8 Configuring the XPR Import Script

After you have installed the import script for the XPR server FI APL you need to configure this script. Its task is to automatically import files from the storage directory just created into the XPR server.

Start the configuration

How to configure the FI APL import script:

- 1) Open the XPR monitor and log on with an administrator account.
- 2) In the modules window of the XPR monitor select **<Settings> – FiApl – Set Options**.

The FI APL configuration dialog opens.

- 3) Switch to the **Protocols** tab.
- 4) Select **Add** and add the FiSym.e script.

The FiSym.e script is now displayed on the **Protocols** tab.

- 5) Mark the FiSym.e script on the **Protocols** tab and select **Properties**.
- 6) Specify the storage directory you have created in [Installing the XPR Import Script](#) on page 285 in the **Poll directory** field.
- 7) In the **Poll rate** field specify the intervals in which the FI APL is to search the poll directory for new files to import them.

Setting **0** (INFINITE) deactivates the automatic search.

A reasonable value would be e. g. 10 seconds.

- 8) Verify that value ***.csv** has been entered in the **header sample** field.
- 9) Select **OK** to copy the settings for the script.
- 10) Select **OK** to copy the settings for the FI APL.
- 11) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

The import script for the FI APL is now configured. The actual import mechanism is now already functional.

4.17.9 Creating an XPR Import File

In the meantime you have configured the import mechanism that will import all UC Application user accounts in the XPR user database.

For the actual import you now need an appropriate import file that contains the relevant information of all UC Application user accounts.

NOTICE: An import file must always contain all UC Application user accounts that are to access OpenScape UC Application via the PhoneMail script. For: A user account of the XPR user database is automatically deleted during the import if it was originally imported from the UC Application system but is not contained in the current import file.

Start the configuration

How to create an import file with all UC Application user accounts:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.
The dialog for exporting configurations opens.
- 4) Select the check box of the component **Domain Management Export for Xpressions**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Open or save the file as usual.
- 8) Click on **Cancel** to close the export window.
- 9) Open the following directory in the exported zip file:
`${exportWorkingDir}`
- 10) In the directory open the following zip file:
`Package_XprDomainmanagement_XprDomainmanagement_01.zip`
- 11) Open the following directory in the zip file: `${BackupAppWorkDir}`
- 12) Save the following file contained therein:
`domain_configuration.csv`
- 13) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems you may have to divide the created import file into different import files. This division depends on how you wish to distribute the user accounts of a UC Application system among the connected OpenScape Xpressions systems. You have performed corresponding plannings in [Planning Details for an \$m \times n\$ Connection](#) on page 274.
- 14) When you configure an $m \times n$ connection with several UC Application systems, you must execute the described steps for all UC Application systems.

You have now created an import file that contains the relevant user information of all UC Application user accounts.

4.17.10 Importing an XPR Import File

The user accounts of the just created import file must now be imported into the XPR user database.

They are imported automatically after you have stored the import file in the APL's storage folder.

IMPORTANT: An import file must always contain all UC Application user accounts that are to access the UC Application system via the PhoneMail script. For: A user account of the XPR user database is automatically deleted during the import if it was

originally imported from the UC Application system but is not contained in the current import file.

IMPORTANT: In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you may have to import the different import files only in selected OpenScape Xpressions systems. You have performed corresponding plannings in [Planning Details for an \$m \times n\$ Connection](#) on page 274.

Start the configuration

How to import the import file with the UC Application user accounts in the XPR user database:

- 1) Configure a system ID to be freely assigned on the OpenScape Xpressions system for the following registry value. This ID should refer to the UC Application system from which the user accounts to be imported originate.

You have performed corresponding plannings in [Planning Details for an \$m \times n\$ Connection](#) on page 274.

HKLM\SOFTWARE\PP-COM\MRS\FiApI\FiSym\ConSrv [REG_SZ]

Example of an environment with a single UC Application system:

UC

Example of an environment with several UC Application systems:

UC1

During the import, this system ID is automatically copied into the XPR database field **CONSRV** for all imported user accounts. The OpenScape Xpressions system will later use this setting to determine the connection data for the OpenScape Web Client of the correct UC Application system in the `param.xml` configuration file. Compare [Configuring the Web APL of OpenScape Xpressions](#) on page 290.

- 2) Copy the just created import file `domain_configuration.csv` to the storage folder you have configured for the import script (cf. [Section 3.18.8, "Configuring the XPR Import Script"](#), on page 566).
- 3) Wait at least as long as you have specified for the import script under **Poll rate** (cf. [Configuring the XPR Import Script](#) on page 286).

The UC Application user accounts have now been imported in the XPR user database.

IMPORTANT: If you import a new user account in the XPR user database that has no PIN or password, the XPR server automatically assigns the relevant user a default PIN or password. The default PIN reads **1111** and the default password **password**. You can change these default values via the registry values **Password** and **Pin** of the FI APL. You find detailed information about the relevant registry values in the *OpenScape Xpressions Server Administration* manual.

- 4) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

4.17.11 Rebooting the XPR Server

You need to reboot the XPR server for the XPR user database settings to take effect.

Start the configuration

How to reboot the XPR server:

IMPORTANT: By the following steps, the XPR server is stopped without any further prompt and immediately restarted. This interrupts the XPR server services.

- 1) Open the XPR monitor and log on with an administrator account.
- 2) From the **start** menu of the Windows operating system select **All Programs – xpr – Stop Server**.
All XPR server services are stopped.
- 3) Wait until you see that all XPR services are stopped in the XPR monitor.
- 4) From the **start** menu of the Windows operating system select **All Programs – xpr – Start Server**.
All XPR server services are started.
- 5) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

You have now rebooted the XPR server. The modifications performed in the XPR user database take effect.

4.17.12 Assigning a Privilege to XPR Users

So that an XPR user can deploy the features of the OpenScape Xpressions connection, an XPR user profile must have been assigned to this user that contains the **Trusted Transfer Mode** privilege. Activate the **Trusted Transfer Mode** privilege in the most simple case in an existing XPR profile that you have already assigned to the relevant XPR users.

You can also create a new XPR user profile that exclusively contains the **Trusted Transfer Mode** privilege and that you assign to the relevant users in addition. How to create a new user profile in the XPR server is described in the *OpenScape Xpressions Web Assistant* manual.

Start the configuration

How to activate the **Trusted Transfer Mode** privilege for XPR users in an existing XPR user profile:

- 1) Start the Web Assistant and log on with an administrator account.
- 2) Select the **User administration** entry in the **Server settings** navigation.
- 3) Specify in the **Find** field the name of the profile for which you want to activate the **Trusted Transfer Mode**.
- 4) Select **Reload**.

You see all entries of the user database that match the entered search criterion.

- 5) Click on the ID of the profile for which you want to activate the **Trusted Transfer Mode**.

You see the settings of the relevant profile.

- 6) Select **Edit**

The dialog with the privileges of the relevant profile opens.

- 7) Select the **Permit** checkbox for the **Trusted Transfer Mode** privilege.
- 8) Select **Apply** to copy the settings for the script.
- 9) Select **Save** to copy the modifications to the user database.
- 10) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

You have now activated the **Trusted Transfer Mode** privilege in the XPR user profile. All XPR users who have been assigned this user profile can now use the OpenScape Xpressions connection.

4.17.13 Configuring the Web APL of OpenScape Xpressions

Users can deploy the OpenScape Web Client for accessing their voicemails in the OpenScape Xpressions system or configuring various private XPR system settings. This requires configuring the OpenScape Xpressions Web APL.

Start the Web APL configuration

How to configure the OpenScape Web Client connection data for the OpenScape Xpressions Web APL:

IMPORTANT: By the following steps, the OpenScape Xpressions Web APL is stopped without any further prompt and immediately restarted. This interrupts the Web APL services.

- 1) Open a Windows command prompt on the OpenScape Xpressions computer system and stop the OpenScape Xpressions Web APL with the following command.

```
net stop webapl
```

- 2) Open the following configuration file on the OpenScape Xpressions computer system:

```
param.xml
```

You find this file in the following directory:

```
<XPR-Install13>\res\WebAp\WebAdmin\
```

In this configuration file the connection data for the OpenScape Web Client of a UC Application system is formatted as follows:

<param id="ComAssistantSSLMode-<system ID >">	
	true
</param>	

¹³ <XPR-Install > is the setup directory of the OpenScape Xpressions system.

<param id="ComAssistantCert-<system ID >">	
	cacert.pem
</param>	
<param id="ComAssistantAddress-<system ID >">	
	<IP address of the OpenScale Web Client>
</param>	
<param id="ComAssistantPort-<system ID >">	
	<port number of the OpenScale Web Client >
</param>	

The **<system ID >** specification may serve for differentiating connections to different UC Application systems. It must correspond to the value you have specified for the **CONSRV** database field of the relevant XPR users (cf. [Importing an XPR Import File](#) on page 287).

In case of an $m \times n$ connection of OpenScale Xpressions and UC Application systems with several UC Application systems, one connection must have been configured to each of the connected UC Application systems.

- 3) Configure the configuration data for each UC Application system to be connected to the OpenScale Xpressions system as follows.
 - a) Create an individual configuration section in the above format.
 - b) Specify the same **<system ID >** you have determined for the relevant XPR users in the **CONSRV** database field for all parameters of a section.
 - c) Specify for the **ComAssistantAddress** parameter the IP address under which the OpenScale Web Client of the relevant OpenScale Xpressions system can be reached.
 - d) Specify port number 7789 for the **ComAssistantPort** parameter.

Example of an OpenScale Xpressions system to which UC Application systems are connected. For all XPR users to deploy the first UC Application system value UC1 has been determined for the CONSRV database field. For all XPR users to deploy the second UC Application system value UC2:

```
<param id="ComAssistantSSLMode-UC1">
    true
</param>
<param id="ComAssistantCert-UC1">
    cacert.pem
</param>
<param id="ComAssistantAddress-UC1">
    10.11.10.1
</param>
<param id="ComAssistantPort-UC1">
    7789
</param>

<param id="ComAssistantSSLMode-UC2">
```

```
        true
    </param>
    <param id="ComAssistantCert-UC2 ">
        cacert.pem
    </param>
    <param id="ComAssistantAddress-UC2 ">
        10.11.10.2
    </param>
    <param id="ComAssistantPort-UC2 ">
        7789
    </param>
```

- 4) Save the changes in the configuration file.
- 5) Start the OpenScape Xpressions Web APL with the following command:

```
net start webapl
```
- 6) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

NOTICE: Keep in mind that not every OpenScape Xpressions system is necessarily connected to the same UC Application systems. You have planned the OpenScape Xpressions and UC Application systems' networking structure in [Planning Details for an \$m \times n\$ Connection](#) on page 274.

4.17.14 Configuring PhoneMail Script Settings

Users can deploy the OpenScape Web Client for accessing their voicemails in the OpenScape Xpressions system or configuring various private XPR system settings. This requires configuring the PhoneMail script settings of OpenScape Xpressions.

Start the configuration

How to configure the PhoneMail script settings of OpenScape Xpressions:

- 1) Open in the XPR monitor the settings dialog for the telematics APL used.
- 2) Switch to the **Protocols** tab.
- 3) Doubleclick the **Xpressions PhoneMail** entry.
The properties dialog of the E-protocol opens.
- 4) Switch to the **Script** tab.
- 5) Select **Parameters**.
The dialog for configuration parameters opens.
- 6) Switch to the **Customer** tab.
- 7) Enter the **-con** value under **Parameters**.
- 8) Select **OK** to copy the parameter setting.
- 9) Close all configuration dialogs of the telematics protocol.
- 10) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

4.17.15 Creating a UC Application Import File

To ensure a smooth OpenScape Xpressions connection, OpenScape Xpressions-related **##ExternalId** entries must be configured for all UC Application user accounts in the UC Application user database. You do this by importing an import file that contains all required user data and that can be directly exported from the OpenScape Xpressions system.

Start the configuration

How to export the import file for the UC Application user database from the OpenScape Xpressions system:

- 1) Execute the following command in the command line of the OpenScape Xpressions system in one line:

```
Infotool export rec=UC_USER file=<file path>\<name of the import file>.txt srv=<CONSRV value>
```

Value **<CONSRV value>** determines that only the XPR user accounts for which the **CONSRV** database field has value **<CONSRV value>** are exported.

Example:

```
Infotool export rec=UC_USER file=import_uc1.csv srv=UC1
```

In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you are thus enabled to export only the XPR user accounts assigned to an individual UC Application system.

- 2) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must create an individual import file that contains exclusively the XPR user accounts related to the respective UC Application system for each UC Application system.

To restrict the export accordingly, you must set value **<CONSRV value>** in each infotool command.

- 3) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

You have now created an import file that contains the OpenScape Xpressions related **##ExternalId** entries for the UC Application user database.

4.17.16 Importing a UC Application Import File

The OpenScape Xpressions-related **##ExternalId** entries of the just created import file must now be imported in the UC Application user database.

IMPORTANT: In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you may have to import the different import files only in selected UC Application systems. Which systems are concerned results from your plannings in [Planning Details for an \$m \times n\$ Connection](#) on page 274.

Start the configuration

How to import the import file with the XPR user accounts in the UC Application user database:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.
The dialog for importing configurations opens.
- 4) Select under **Import file** the csv-based import file with the XPR user data to be imported.
- 5) Click on **Next**.
- 6) Select under **Type of file to be imported** the **Common Management Platform** option.
- 7) Select under **Included type of data** the **Domain Management** option.
- 8) Click on **Import**.

The data import starts. A message indicates the end of the data import.

- 9) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must execute the described steps on all UC Application systems.

The XPR user accounts are now imported in the UC Application user database.

4.17.17 Configuring OpenScape Web Client

Users can deploy the OpenScape Web Client for accessing their voicemails in the OpenScape Xpressions system or configuring various private XPR system settings. This requires configuring the OpenScape Web Client.

Start the configuration

How to configure the OpenScape Web Client:

- 1) Open the following configuration file on the OpenScape UC Application computer system:

voicemail.xml

You find this file in the following directory:

`<Osc-Install14>/HiPathCA/config/common/`

NOTICE: In former OpenScape UC Application versions, the `xpressions.cfg` configuration file was used to configure a connection to OpenScape Xpressions. In this file, however,

¹⁴ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

you cannot configure several OpenScape Xpressions connections. Therefore, always use the `voicemail.xml` configuration file for fresh installations. You can still use the `xpressions.cfg` configuration file for upgrades as long as you do not wish to connect several OpenScape Xpressions systems to OpenScape UC Application.

2) Configure in the configuration file the following bolded settings.

```
<xpressions>

<xpressionsServer> <!-- The name of the server -->
<!-- The name of the server -->
  <name><assignedExternalSystemId  of the OpenScape
Xpressions system ></name>
  <!-- The server address which is visible to the
browsers - required to
provide user access to the Xpressions configuration
dialog.
Please use one of the formats
...
example: <address>http://xpressions.mycompany.com</
address> -->
  <address>https://< URL of the Web Assistant></address>
  <!-- The IP address used by the xprproxy service to
access the Xpressions server
example: <remoteIpAddr>127.0.0.1</remoteIpAddr> -->
  <remoteIpAddr>< IP address of the XPR computer
system with Con APL > </remoteIpAddr>
  <!-- The port on which the Xpressions server listens
for requests
from the xprproxy service -->
  <remotePort>10000</remotePort>
</xpressionsServer>
</xpressions>
```

NOTICE: You can determine `assignedExternalSystemId` of the *OpenScape Xpressions system* e. g. in one of the UC Application import files you have exported from the associated OpenScape Xpressions system in [Creating a UC Application Import File](#) on page 293.

3) If you use OpenScape Xpressions version 5, configure the following setting in addition.

```
<!-- The port on which the Xpressions server listens for
requests from the xprproxy service -->
<remotePort>10000</remotePort>
```

This is a default setting of OpenScape Xpressions version 6. Specify another port number here only if you change this setting in OpenScape Xpressions accordingly.

4) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you

must configure the connection data for each of the relevant OpenScape Xpressions systems.

To do this, add a section of the following format for each further OpenScape Xpressions system in the configuration file:

```
<xpressionsServer>
  <name><assignedExternalSystemId  of the OpenScape
  Xpressions system ></name>
  <address> https://< URL of the Web Assistant > </
address>
  <remoteIpAddr> < IP address of the  XPR  computer
system with Con APL > </remoteIpAddr>
  <remotePort> 10000 </remotePort>
</xpressionsServer> -->
```

NOTICE: There should be no trailing slashes

- 5) Save the changes in the configuration file.
- 6) Open the following configuration file on the OpenScape UC Application computer system:

JrnService.cfg

You find this file in the following directory:

<Osc-Install¹⁵>/HiPathCA/config/services/default/JrnService

- 7) Configure the following setting in the configuration file.

voiceMailDevices=<phone number>[,<phone number>]

List all phone numbers (separated by comma) the communications system uses to forward calls to OpenScape Xpressions. In doing so, use the normalized phone number format without special characters.

Example: 4924049011234

- 8) Save the changes in the configuration file.
- 9) In case of an m × n connection of OpenScape Xpressions and UC Application systems with several OpenScape Xpressions systems you must execute the described steps on all OpenScape Xpressions systems.

4.17.18 Changing UC Application User Profiles

The settings of the default user profiles **Essential**, **Professional** and **Team** are configured in a way that the relevant users deploy the integrated voicemail feature OpenScape UC Application as voicemail system.

If you wish to use OpenScape Xpressions as voicemail system, you need to change the user profiles accordingly. But because the default profiles **Essential**, **Professional** and **Team** are write-protected, you must create a copy of each of the available profiles to change their settings.

You need to assign the thus changed user profiles to the users who are to deploy OpenScape Xpressions as voicemail system at a later date.

¹⁵ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

Start the configuration

How to create copies of the default user profiles **Essential**, **Professional** and **Team** and change their settings for the voicemail system used :

- 1) Select in the **Domain** drop-down list of the CMP toolbar the domain the user profiles of which you wish to copy.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **CMP** menu item on the **Configuration** navigation tab of the CMP.

- 3) In the navigation tree, click on **General > Profiles**.

A list of all profiles configured in the selected domain appears in the workspace.

Tick off the check box of the **Essential** profile.

- 4) Click on **Copy**.

The dialog with the settings of the profile copy opens.

- 5) Change the text **Copy of Essential** under **Name** to a short, unique name for the new profile – e. g. **Essential – XPR-Voicemail**.

Under this name the profile is administered in the CMP.

- 6) Select the check box for the privilege **Essential > Voice Mail Access via ... > ...via Xpressions**.

- 7) Untick under **Essential > Voice Mail Access via ...** all other check boxes.

- 8) Click on **Save** to copy the settings.

The new user profile is saved and displayed in the profiles list.

- 9) Execute steps 4 to 9 also for the default user profiles **Professional** and **Team**.

- 10) In case of an $m \times n$ connection of OpenScape Xpressions and UC Application systems with several UC Application systems you must execute the described steps on all UC Application systems.

You have now created user profiles that determine OpenScape Xpressions as voicemail system.

You need to assign the thus changed user profiles to the users who are to deploy OpenScape Xpressions as voicemail system at a later date.

As soon as you have assigned one of the changed profiles to a user, this user will see the tab for accessing OpenScape Xpressions voicemails in the OpenScape Web Client. Displaying this tab is independent from whether or not connections to OpenScape Xpressions systems have been configured in the voicemail.xml (or xpressions.cfg) configuration file.

OpenScape Xpressions is now connected to OpenScape UC Application.

4.17.19 Nuance services to be verified to allow simultaneous availability of WebAssistant and the Voice Mail tab in WebClient

If started, the Nuance Watcher Daemon (nuance-wd) changes a kernel parameter every Linux start. This parameter prevents simultaneous availability of WebAssistant and the Voice Mail tab in WebClient.

The setting set by nuance-wd is the following:

net.ipv4.tcp_tw_recycle=1

And it should not be "1". It should be the Linux default value, which is "0".

Nuance Watcher is installed as part of the Speech Server installation, but by default it is not started and is not required.

After the installation the service should be disabled, otherwise when the server is rebooted nuance-wd service will run, change the kernel parameter and lead to the behavior mentioned. To do this:

Double check that the service is not running (needs root privileges)

```
#service nuance-wd stop
```

To disable the service

```
#chkconfig --level 345 nuance-wd off
```

To remove it from the startup list, use the --del option as shown below:

```
#chkconfig --del nuance-wd
```

After that please check if the script "nuance-wd" still on the server and delete it manually.

Please plan a reboot of the server and check again the kernel settings. If necessary, change them to "0" again.

4.18 Configuring the System Networking

NOTICE: You need to execute the configuration steps of this chapter only if you use the deployment scenario Very Large Deployment or network other deployment scenarios with each other. This configuration is required for the presence and instant-messaging functions to work across systems.

With Very Large Deployment you can install OpenScape UC Application with several networked clusters for providing the UC Application services to a maximum number of users.

If required, all other deployment scenarios of OpenScape UC Application can be networked with help of the Openfire system's Federation functionality also. This is useful, for example, to connect UC Application environments operated separately so far in the scope of a company merger, thus providing the users of both UC Application environments with presence information.

How to configure the cluster networking for Very Large Deployment or the networking of other deployment scenarios:

- 1) [Configuring the Openfire Server](#)
- 2) [Configuring the Conference Portal](#)
- 3) [Configuring the Size of the JVM Heap](#)

These steps are described in detail in the following sections.

4.18.1 Configuring the Openfire Server

IMPORTANT: Before you execute the configuration steps for the system networking of single deployment scenarios you must have completed preparatory configuration steps. These are described in the *OpenScape UC Application, Installation and Upgrade* manual.

NOTICE: The following configuration assumes that you network Very Large Deployment or other deployment scenarios with help of several Openfire servers. Even if the number of users does not explicitly demand this networking at the time of the installation, it is useful for preparing the UC Application system for a growing number of users in advance. This requires more than one Openfire server having already been installed. If, in contrast, you wish to use Very Large Deployment or other networked deployment scenarios with a single Openfire server, you can configure this Openfire server as described in [Configuring the Openfire Server](#) on page 299.

NOTICE: You have performed an initial configuration for each Openfire server during the OpenScape UC Application setup. You have now assigned an application computer to each Openfire server. To configure an individual Openfire server in the following, you need to open the CMP on an application computer assigned to the desired Openfire server.

You configure the Openfire server via the web-based Openfire administration interface. You can start this administration interface in the CMP via the configuration dialog for presence and instant messaging.

Start the configuration

Configure one Openfire server by executing the following steps on the relevant application computer.

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Presence & IM**.

The configuration dialog for presence and instant messaging opens.

- 3) Select **Start Openfire Admin UI**.

The login dialog for the administration interface of the Openfire server opens.

NOTICE: The **Start Openfire Admin UI** button is only active if the connection data for the Openfire server was configured and tested. This should have been done during the OpenScape UC Application setup.

- 4) Log on to the Openfire server under an administrator account.

In doing so please note:

- After a new installation of the Openfire server, the following default password is valid for the user accounts **administrator** and **admin**:

Asd123!.

- After an upgrade, the following default passwords are valid:
 - For the user account **administrator**, the default password is:
8ABWnmppzEOuxu1q
 - For the user account **admin**, the default password is:

01*Test!

NOTICE: The valid passwords can be changed individually on the Openfire administration interface. You find details about this in the Openfire server product documentation.

The Openfire administration interface opens.

- 5) Switch on the **Server** tab to **Server Settings** and select the menu option **Server to Server**.
- 6) Ensure that the **Never close idle connections** option under **Idle Connections Settings** is active.
- 7) If you have changed the setting, select **Save Settings** under **Idle Connections Settings**.
- 8) Activate under **Allowed to Connect** one of the following options.
 - **Anyone**, to allow the connection to any Openfire server.
 - **White List**, to allow only the connection to selected Openfire servers.
- 9) If you have changed the setting, select **Save Settings** under **Allowed to Connect**.
- 10) If you have activated the **White List** option under **Allowed to Connect**, specify the following under **Domain**:
 - The XMPP domain name of the Openfire servers that the local Openfire server may connect.
Example: openfire1
 - The fully qualified conference service name of the Openfire servers that the local Openfire server may connect.
The name of a conference service has the following format:
conference.<domain name>
Example: conference.openfire1
- 11) Select the **HTTP Binding** menu option.
- 12) Ensure that the **Disabled – Clients will not be able to connect with this server using HTTP bindings** option is active.

NOTICE: OpenScape UC Application connects to the Openfire server via the XMPP protocol only.

- 13) If you have changed the setting, select **Save Settings**.
- 14) Select the **Registration & Login** menu option.

- 15) Ensure that the **Disabled – Users can not automatically create new accounts** option under **Inband Account Registration** is active.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 16) Ensure that the **Disabled – Users are not allowed to change their password** option under **Change Password** is active.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 17) Ensure that the **Disabled – Only registered users may login** option under **Anonymous Login** is active.

NOTICE: If this feature is active, it may disrupt the automatic synchronization between OpenScape UC Application and Openfire server.

- 18) If you have changed a setting, select **Save Settings**.

- 19) Select the **Offline Messages** menu option.

- 20) Ensure that any of the following options under **Offline Message Policy** is active:

- **Bounce – Never store offline messages and bounce messages back to the sender.**
- **Drop – Never store offline messages and drop messages so the sender is not notified.**

NOTICE: OpenScape clients dismiss messages about message deletion (bounce messages). The behavior of the OpenScape clients is thus the same for both options.

- 21) If you have changed the setting, select **Save Settings**.

- 22) Select the **Private Data Storage** menu option.

- 23) Ensure that the **Disabled Private Data Storage – Do not allow server-side storage** option under **Set Private Data Policy** is active.

NOTICE: This feature is not supported by OpenScape clients.

- 24) If you have changed the setting, select **Save Settings**.

- 25) Select the **File Transfer Settings** menu option.

- 26) Ensure that the **Disabled – This server will not act as a file transfer proxy** option under **Proxy Service** is active.

NOTICE: This feature is not supported by OpenScape clients.

- 27) If you have changed the setting, select **Save Settings**.

- 28) Select the **Search Service Properties** menu option.

- 29) Ensure that the **Disabled – Clients will not be able to search for users** option under **Service Enabled** is active.

NOTICE: This feature is not supported by OpenScape clients.

- 30) If you have changed the setting, select **Save Properties**.
- 31) Perform the described settings for each of the Openfire servers used.
- 32) Adjust the `hosts` file of each Openfire computer system or an available DNS server as follows.
- a) Verify that each Openfire server can resolve the fully qualified domain names (FQDN) and the XMPP domain names of the respectively other Openfire servers in an IP address correctly.

NOTICE: We recommend to use identical names for the fully qualified domain name (FQDN) and the XMPP domain name of an Openfire server.

- b) Verify that each Openfire server can resolve the fully qualified conference service names of the respectively other Openfire servers in an IP address correctly. The name of a conference service has the following format:

`conference.<domain name>`

Example: conference.openfire1

NOTICE: You find the `hosts` file on a Linux-based computer system in directory `/etc/`.

You have now configured the Federation functionality of the Openfire server for networking.

4.18.2 Configuring the Conference Portal

In a networked system environment the conference participants of another UC Application cluster or of a networked deployment scenario can only access a restricted conference call control. This conference call control can be reached via an individual URL. If this URL shall be sent in the e-mail notifications of the conference portal, it must be configured for the e-mail notifications.

Start the configuration

Configure the URL of the restricted conference call control for e-mail notifications by executing the following steps on the relevant application computer:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.
- 3) The configuration dialog of the conference portal plugin opens.
- 4) Switch to the **Misc** tab.
- 5) Select the **Notification settings** link.

- 6) Enter under **URL Configuration** the URL under which the OpenScape Web Client of the local UC Application cluster or of the local deployment scenario can be reached.

Example: http://172.0.0.1:7789

- 7) Configure the URL on each application computer in this way.

You have now configured the conference portal for a networked system environment.

4.18.3 Configuring the Size of the JVM Heap

To optimize the system performance for exchanging presence information we recommend to adjust the size of the JVM Heap on all application computer.

Start the configuration

Configure the size of the JVM Heap by executing the following steps on each application computer:

- 1) Open the following configuration file on the relevant application computer:

`DaemonConfig.xml`

You find this file in the following directory:

`<Osc-Install16>/common/conf/`

- 2) Find the following section in the configuration file:

```
<Item guid="FrameworkContainer"
name="FrameworkContainer">
```

- 3) Change the parameters

```
-Xms1920m -Xmx1920m -Xmn256m -Xmo1664m
```

as follows:

```
-Xmx2560m -Xms2560m -Xmo2048m -Xmn512m
```

- 4) Save the changes in the configuration file.
- 5) Change the described configuration file on each application computer.

You have now performed all settings required for a networked system environment.

4.19 Configuring Inbound / outbound device

With V11 the default behaviour is when the device is changed, only the incoming device (inbound call) is changed. The outgoing device (outbound call) remains as it is.

In order to get the old behavior (inbound and outbound call are changed) you have to set in CMP the property **Set Inbound Preferred Target** only from true to false.

In order to do this, go to CMP

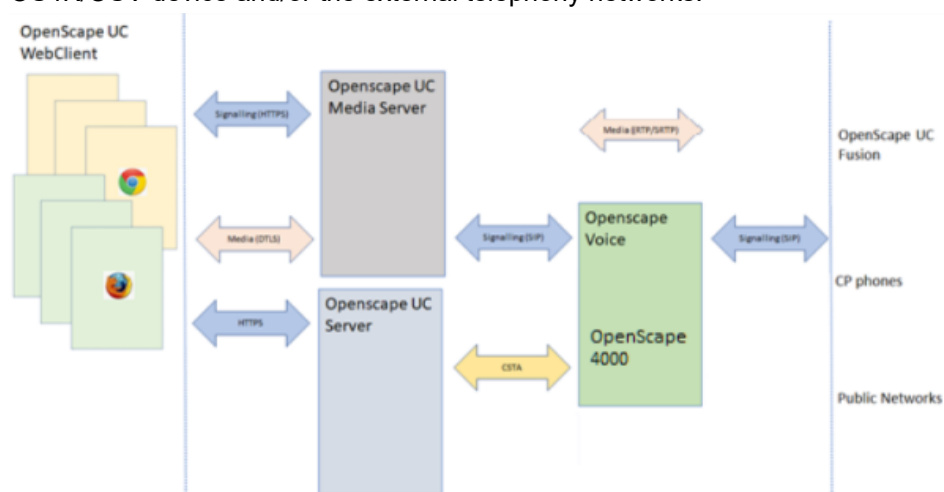
¹⁶ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 1) **CMP > Maintenance > Inventory > Nodes**
- 2) Select the UC Application Node (this node is of type **Application**)
- 3) In the dialog that opens, click **Show** for the **Show Service Status**
- 4) Select the setting **Automation - Presence Based Target Definition** and change the property **Set inbound Preferred Target only** from true to false.

4.20 Configuring WebRTC functionality

In OpenScape UC V11, you can create WebRTC with OpenScape 4000 (OS4K) or devices registered to OSV and controlled in the same way as other devices (CP phones or softphones). The WebRTC devices in UC V11 provide audio/video(H264) capabilities for users operating UC features through Chrome and Firefox (in Microsoft Windows, MAC or Linux OS).

Every WebRTC endpoint is connected to the OpenScape Media Server that registers an exclusive SIP subscriber in OSV/OS4K to be used as ONS or OND by the user. Thus, OpenScape UC is capable of controlling this device via CSTA protocol. Furthermore, this WebRTC device can communicate with any other OS4K/OSV device and/or the external telephony networks.



4.20.1 Prerequisites

The following are basic prerequisites for using the WebRTC functionality:

- Functional UC V11 R1 (Standard Duplex Small, Large or Very Large Deployment).
- Maximum number of WebRTC users is 20 (Small deployment) and 350-1000 (Large or Very Large deployment).
- Valid server certificate and its private key issued by the MS node by a trusted Root CA.
- The Root CA certificate.
- WebRTC licenses.
- Xpressions must have the fix "Telematic-811FR5-20337".
- Chrome, Microsoft Edge (Chromium based) or Firefox browser in the user machines.
- HAProxy (for internet usage)

Additional Prerequisites for WebRTC connected to OpenScape 4000:

- RMX V11 R0.28.9
- Assistant / Manager V11 R0.28.3
- Specific LW-Hotfix V11 R0.28.2

WebRTC with OpenScape 4000 is supported starting with UC 10R2 FR2.

In case of ONS/OND WebRTC setup the OND (SIP) has to be configured on the same system with the ONS device.

IMPORTANT: After upgrading from a version lower than V11 R0.28.3 to a version greater or equal to V11 R0.28.3, an upload all in assistant/manager is necessary in order to populate database with needed parameters of WebRTC feature for already created SIP/UFIP stations. After that, a full synchronization of upgraded nodes is required in UC CMP under Maintenance > Inventory > Nodes

4.20.2 Restrictions

The following restrictions apply to the WebRTC functionality:

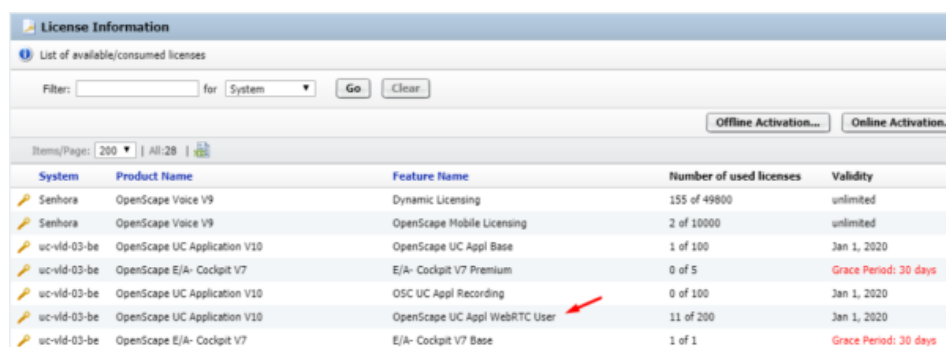
- Control of Audio device buttons is not available
- Pickup groups are not supported.
- Only Chrome and Microsoft Edge Chromium are supported
- Mozilla Firefox can be used with following restrictions
 - Only with Windows default audio device
 - Required manual refresh after network changes
 - Notifications toaster does not provide answer / decline buttons.
- Limited Mode is not supported (OSB).
- OSMO swipe feature is not supported.
- Click to Dial is not supported.
- TURN with IPV6 is not supported.

Additional Restrictions for WebRTC connected to OpenScape 4000:

- Hold/retrieve not supported
- SIP subscriber not supported
- Second call for WebRTC
- The UC WebRTC users functionality is supported only on OpenScape 4000 STMIX boards and SoftGate (virtual HG). STM12 and STM14 boards are not supported for WebRTC functionality

4.20.3 WebRTC licenses

WebRTC licenses are required for the installation. OpenScape UC V11 supports up to 1000 licenses depending on your deployment (small, large or very large). For more information regarding required WebRTC licenses depending on your deployment, please refer to the OpenScape UC V11 Planning Guide Chapter 7.9.3 Planning required WebRTC licenses.



License Information

List of available/consumed licenses

Filter: for System

Items/Page: 200 | All: 28

System	Product Name	Feature Name	Number of used licenses	Validity
Senhora	OpenScope Voice V9	Dynamic Licensing	155 of 49800	unlimited
Senhora	OpenScope Voice V9	OpenScope Mobile Licensing	2 of 10000	unlimited
uc-vld-03-be	OpenScope UC Application V10	OpenScope UC Appl Base	1 of 100	Jan 1, 2020
uc-vld-03-be	OpenScope E/A- Cockpit V7	E/A- Cockpit V7 Premium	0 of 5	Grace Period: 30 days
uc-vld-03-be	OpenScope UC Application V10	OSC UC Appl Recording	0 of 100	Jan 1, 2020
uc-vld-03-be	OpenScope UC Application V10	OpenScope UC Appl WebRTC User	11 of 200	Jan 1, 2020
uc-vld-03-be	OpenScope E/A- Cockpit V7	E/A- Cockpit V7 Base	1 of 1	Grace Period: 30 days

4.20.4 Configuring WebRTC in OSV

You must create SIP subscribers in OSV for every UC WebRTC device. This allows OpenScope UC to control WebRTC devices via the CSTA protocol in the same way it does for other CP phones or Fusion softphones connected to OSV.

From UC V11R5 FR8, Digest Authentication is supported by UC WebRTC devices. Therefore, the steps described in chapters [Configuration of trusted list in OSV](#) on page 306 and [Configuration of trusted subscribers](#) on page 307 are optional.

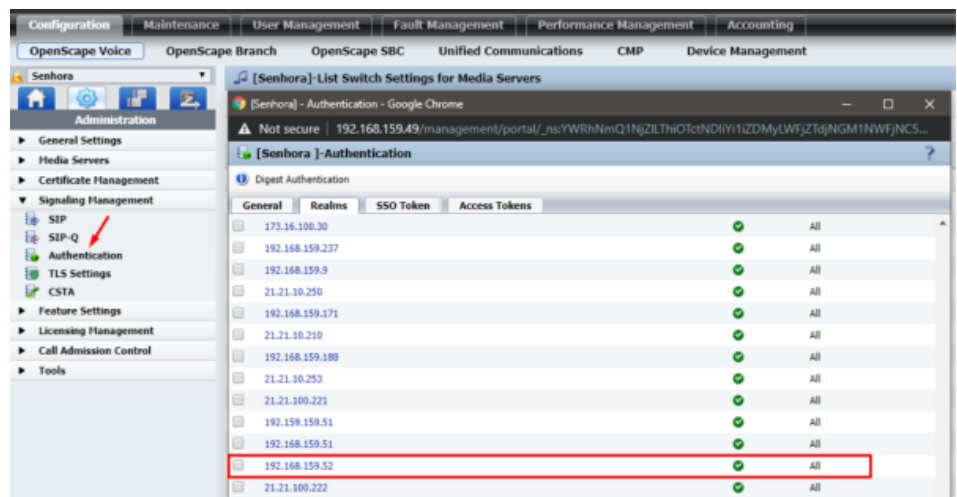
4.20.4.1 Configuration of trusted list in OSV

In the CMP platform add the IP address of the Media Server node to the OSV's trusted list.

IMPORTANT: It is highly recommended to use Digest Authentication.

- 1) In CMP, navigate to Configuration > OpenScope Voice > Administration > Signaling Management > Administration.
- 2) In the Realms tab click Add.
- 3) A pop-up window appears. Configure the IP address of the Media Server node and click Save.

The IP address of the Media Server node has been added to OSV's trusted list.

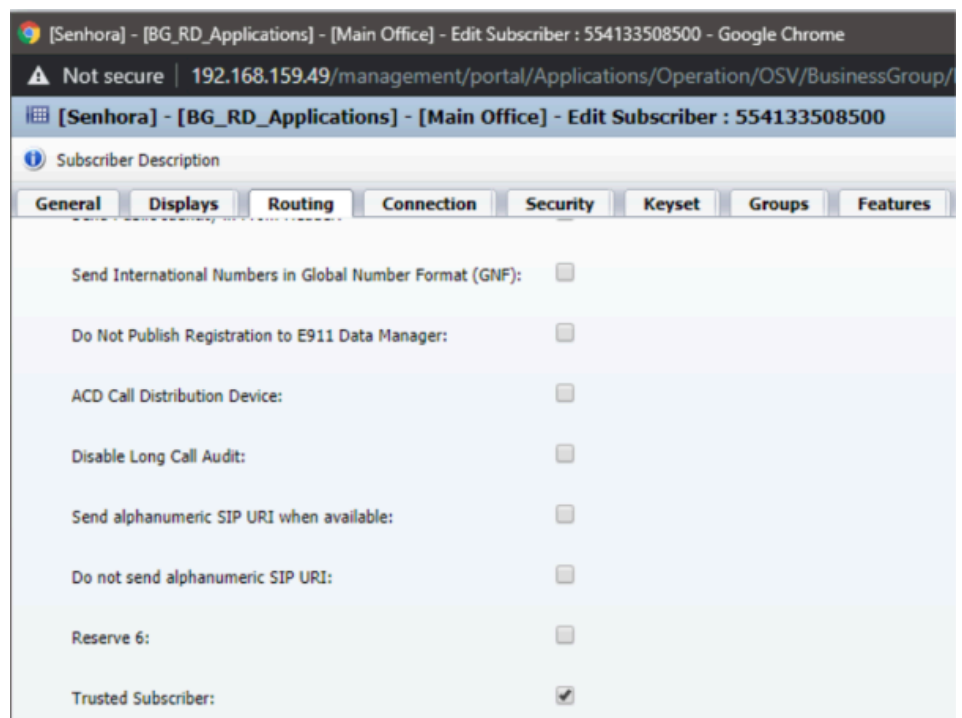


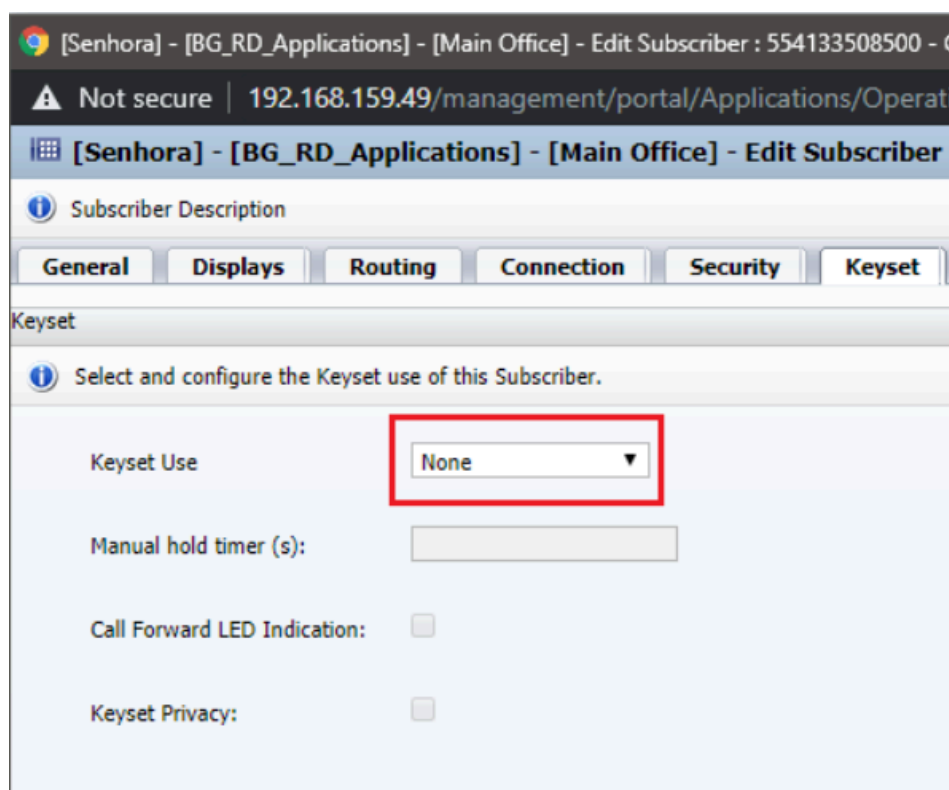
4.20.4.2 Configuration of trusted subscribers

OpenScope Media Server registers a SIP subscriber for each WebRTC endpoint.

Mark all subscribers of Media Server as Trusted, as they are used for communication between two servers (Media Server and OSV) in an internal network and therefore they are allowed to bypass Digest Authentication.

- 1) In CMP, navigate to Configuration > OpenScope Voice > Business Groups > Members.
- 2) Select Edit Subscriber.
- 3) In the Routing tab, check the Trusted Subscriber option.
- 4) Select None in the Keyset Use option list of the Keyset tab.





4.20.5 Configuring WebRTC with a multiple Media Server system

With V11R2 you no longer have the limitation of using a single Media Server node for the WebRTC functionality. You can use multiple Media Server nodes (up to 5) and these can be accessible outside the corporate network.

In order to do this, you need to configure the following properties in CMP:

- 1) **CMP > Maintenance > Inventory > Nodes**
- 2) Select the UC Application Node (this node is of type **Application**).
- 3) In the dialog that opens, click **Show** for the **Show Service Status**.
- 4) Select the setting **Edit Service Configuration - WebRTC MS Service** and configure the following properties for every node:
 - a) **TURNServerURLs**: Define the TURN URL per Media Server node.
 - b) **MediaServerExternalURL**: Define the external URL of the Media Server node.

NOTICE: If the administrator performs any change to the Transport Protocol (TCP), it is strongly recommended that the WebRTC UC user is prompted to sign out and sign in again, in the application, to avoid functionality implications.

4.20.6 Configuring WebRTC in UC

To configure the WebRTC functionality in UC V11 you have to create and replace the certificates in your servers. The process is separated in two

sections. First you have to create the certificates for the Back End (BE) server. Then you can copy these certificates into the Media Server (MS) and the Front End (FE) servers. You can do so by following the steps described in the sections below.

Before doing any work on the UC servers, take a snapshot of all the VMs used in your setup.

- 1) For end user PC go to C:\Windows\System32\drivers\etc and copy the IPs and FQDNs in the hosts file. For example:

10.10.153.2 UCVL-BE.h8k.sec

10.10.153.3 UCVL-FE.h8k.sec

10.10.170.191 FacadeHA

- 2) Save the hosts file.

IMPORTANT: Due to the DTLS protocol that WebRTC uses to communicate with the UC Media Server, the Media Server must be configured in Secure Only or Secure Preferred mode. You can do this via CMP by navigating to Unified Communications > Media Server > Streaming-IVR and choosing one of the aforementioned security modes.

4.20.6.1 Configuration of certificates in BE server

- 1) Go to /opt/siemens/HiPathCA/distribution/ and create two configuration files ca_config.cnf and server_config.cnf with the following content:

- ca_config.cnf

```
#CA configuration file
#
HOME = .
[req]
default_bits = 2048
default_md = sha256
distinguished_name = req_distinguished_name
x509_extensions = v3_ca

[ req_distinguished_name ]
countryName = US
countryName_default = US
countryName_min = 2
countryName_max = 2
StateOrProvinceName = State
localityName = Locality
organizationName = Organization Name (Company)
organizationalUnitName = Organizational Unit Name (section)
commonName = *.h8k.sec
commonName_max = 64

[ v3_ca ]
keyUsage = keyCertSign, cRLSign
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:true
#EOF
```
- server_config.cnf

```
# Server configuration file. If you are creating certificates for more than
one server

# and are using subAltName then you should create a copy of this file for
each server.

#
HOME = .
[req]
```

```

default_bits = 2048
default_md = sha256
distinguished_name = req_distinguished_name
x509_extensions = v3_req

[ req_distinguished_name ]
countryName = US
countryName_default = US
countryName_min = 2
countryName_max = 2
StateOrProvinceName = State
localityName = Locality
organizationName = Organization Name (Company)
organizationalUnitName = Organizational Unit Name (section)
commonName = *.h8k.sec
commonName_max = 64

[ v3_req ]
keyUsage = keyEncipherment, digitalSignature, nonRepudiation
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:false
# README: If you decide to use subjectAltName you must uncomment
# the following line and AT LEAST one of the lines under [alt_names].
subjectAltName = @alt_names
[alt_names]
# You can define more DNS, IP, URI names etc. Just follow the order.
DNS.1 = *.h8k.sec
# DNS.1 = www.fmm.com
# URI.1 = https://plm.com
#IPs of the BE server:
IP.1 = 10.10.153.2
IP.2 = 10.10.153.3
# IP.2048 = 001:0db8:85a3:0000:0000:8a2e:0370:7334
# EOF

```

NOTICE: The DNS entry *.h8k.sec is different for each customer. It is the domain where all the VMs belong to,

with an asterisk (*) as the wildcard, and the IPs, are the IPs of all the VMs in the system.

2) Create the root CA certificate:

```
openssl req -new -x509 -keyout cakey2023.pem -out cacert2023.pem -nodes -days 3650 -config ca_config.cnf
```

3) Create the key and signing request:

```
openssl req -new -keyout server1key2023.pem -out server1req2023.pem -nodes -config server_config.cnf
```

4) Sign the request using the CA certificate and key created in the previous steps:

```
openssl x509 -req -CA cacert2023.pem -CAkey cakey2023.pem -CAcreateserial -extfile server_config.cnf -extensions v3_req -in server1req2023.pem -out server1cert2023.pem -days 1825
```

5) View your newly created server (not CA) certificate:

```
openssl x509 -text -noout -in server1cert2023.pem
```

6) Now you have these three certificates:

CA = cacert2023.pem

ServerCert = server1cert2023.pem

ServerKey = server1key2023.pem

7) Create the PKCS12 file:

```
openssl pkcs12 -export -in server1cert2023.pem -inkey server1key2023.pem -chain -CAfile cacert2023.pem -name "ms-tomcat" -out pkcs12.p12
```

NOTICE: Keep the alias as ms-tomcat and when asked, keep the password as changeit.

8) Backup the existing keystore before updating it:

```
cp .keystore .keystore_backup
```

9) Use the PKCS12 file that you created to overwrite the existing keystore:

```
cp pkcs12.p12 .keystore
```

NOTICE: Remember to import the CA certificate in the user machines.

4.20.6.2 Importing the certificates and private key to the keystore of the Media Server and Front End servers

Go to all the MS and FE servers and copy the three certificates files from the BE server. These certificates should be copied to the following paths:

```
/etc/ocsinventory/cacert2023.pem
```

```
/etc/ocsinventory/server1cert2023.pem
```

```
/etc/ocsinventory/server1key2023.pem
```

```
/opt/siemens/mediaserver/application_host/providers/tomcat/tomcat-home/conf/cacert2023.pem
```

```
/opt/siemens/mediaserver/application_host/providers/tomcat/tomcat-home/conf/
server1cert2023.pem
```

```
/opt/siemens/mediaserver/application_host/providers/tomcat/tomcat-home/conf/
server1key2023.pem
```

```
/opt/siemens/mediaserver/application_host/work/tomcat-9.0.0/tomcat-home/
conf/cacert2023.pem
```

```
/opt/siemens/mediaserver/application_host/work/tomcat-9.0.0/tomcat-home/
conf/server1cert2023.pem
```

```
/opt/siemens/mediaserver/application_host/work/tomcat-9.0.0/tomcat-home/
conf/server1key2023.pem
```

You will also need to update the Tomcat keystore with the new certificate:

- 1) Go to /opt/siemens/mediaserver/application_host/providers/tomcat/tomcat-home/conf/
- 2) Create the PKCS12 file, keeping the alias as ms-tomcat and the password as changeit:

```
openssl pkcs12 -export -in server1cert2023.pem -inkey server1key2023.pem
-chain -CAfile cacert2023.pem -name "ms-tomcat" -out pkcs12.p12
```

- 3) Import the PKCS12 file to the tomcat keystore:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -importkeystore -
deststorepass changeit -destkeystore keystore.jks -srckeystore pkcs12.p12 -
srcstoretype PKCS12
```

- 4) Verify that the keystore is working:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -list -v -keystore
keystore.jks
```

- 5) Copy the certificate to the directory of the MS keystore:

```
cp <keystore_filepath> /longhorn/opt/unify/docker/volumes/ucms1-ah-
providers/tomcat/tomcat-home/conf/keystore_MS.jks
```

- 6) Enter the following command to change the user of the directory:

```
chown 10101:10101 /longhorn/opt/unify/docker/volumes/ucms1-ah-
providers/tomcat/tomcat-home/conf/keystore_MS.jks
```

- 7) Add the Keystore filename in CMP:

- Navigate to **Unified Communications > Media Server** in CMP.
- Select the respective media server node configuration dialog.
- In the OpenScape Media Server configuration dialog click on the **Providers** tab and select the **System, Security and Remote Access** link from the provider list.
- Change the **Keystore Filename** under the **Mediaserver Internal Webserver > https** tab.
- Click **Save**.

Perform steps 5-7 for every media server in the list.

- 8) Restart the deployment:

- helm delete uc
- watch kubectl get pods (wait until all pods are terminated)
- helm install uc uchelm-xxx.tgz -f values.yaml

Now you have to import the CA certificate to the keystore of the MS server, to ensure that TLS communication will be possible between MS and OSV

- 1) Go to `/opt/siemens/mediaserver/application_host/providers/tomcat/tomcat-home/conf`
- 2) Copy the CA certificate to the directory of the MS keystore:
`cp cacert2023.pem /opt/siemens/mediaserver/application_host/providers/sip-connectivity/cacert2023.pem`
- 3) Go to `/opt/siemens/mediaserver/application_host/providers/sip-connectivity` and locate the old CA certificate to be removed:
`/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -list -v -keystore tls-keystore.jks -storepass password`
- 4) Delete the old certificate:
`/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -delete -alias CA2023 -keystore tls-keystore.jks -storepass password`
- 5) Import the new CA certificate into the keystore:
`/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -import -trustcacerts -alias CA2023 -file cacert2023.pem -keystore tls-keystore.jks`
- 6) Restart the Media Server:
`/etc/init.d/symphoniad restart`

NOTICE: It is recommended to reboot all servers and restart services

You have to transfer the following certificate to your own PC and/or any other PC that you are planning to login the UC application.

CA = cacert2023.pem

You also have to import this certificate file to your Trusted CA certificates:

- 1) Click on the Start menu.
- 2) Type mmc and open the console.
- 3) Click on the File menu and click Add/Remove Snap-in...
- 4) Double click on Certificates
- 5) Click on Computer Account and click Next
- 6) Select Local computer and click Finish.
- 7) Click OK.
- 8) Right-click on the Trusted Root Authentication Authorities folder and select All Tasks > Import.
- 9) In the Certificate Import Wizard click Next
- 10) Click Browse and change the type to all files.
- 11) Locate your certificate file and click Open and Next
- 12) Click Finish to complete the wizard
- 13) Close the MMC console.

4.20.6.3 JWT token protection

As an administrator, you must ensure that the secret used to sign the JWT token is strong and unique, and generated using a secure source of randomness.

The jwtSecret information on the OpenScape UC media server node should be updated in the following paths:

/opt/siemens/mediaserver/application_host/deployment/webkitrestlet/webkit-restlet.component.xml

and

/opt/siemens/mediaserver/application_host/deployment/paasconnectivity/paas-connectivity.component.xml

4.20.7 Configuring WebRTC in OpenScape 4000

It is required to create SIP subscribers in OpenScape 4000 for every UC WebRTC device. This will allow Openscape UC to control WebRTC devices via CSTA protocol in the same way it does for other CP phones or Fusion softphones connected to OpenScape 4000.

In order to have TLS connection between MS and OpenScape 4000 SIP subscriber security class should be set to CIPHER, for TCP connection security class is set to SECURE.

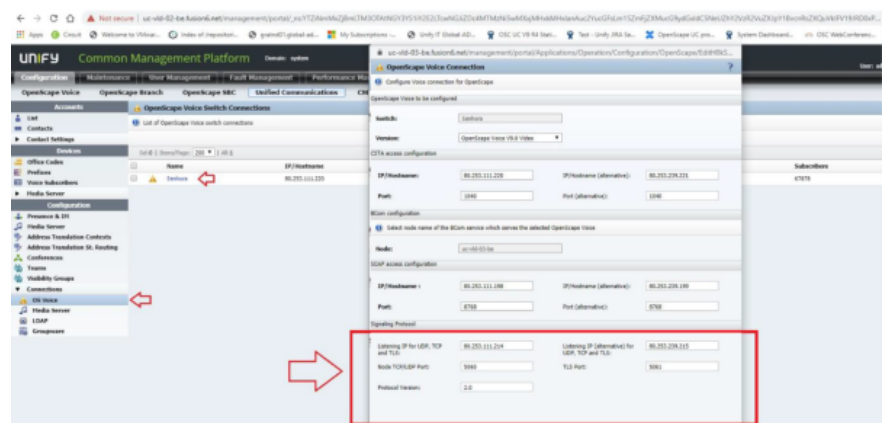
Up to 240 native SIP subscribers can be configured on the common gateway HG 3500 and the virtual HG 3500. The total number of 240 IP subscribers per common gateway (CGW) refers to HFA and SIP subscribers (e.g. 200 HFA and 40 SIP subscribers).

4.20.8 OpenScape Voice Signaling Protocol data synchronization

The OS Voice Signaling protocol data should be replicated in the UC server database.

Double check if these configurations are synchronized in the UC server database in the CMP platform:

- 1) In CMP, navigate to Configuration > Unified Communications > OS Voice > OpenScape Voice Connection.
- 2) In the Signaling Protocol section configure the following parameters with the OpenScape Voice information:
 - a) Listening IP for UDP, TCP and TLS
 - b) Listening IP (alternative) for UDP, TCP and TLS
 - c) Node TCP/UDP Port
 - d) TLS Port
 - e) Protocol Version



4.20.8.1 Singaling Protocol fields are empty

If these fields are empty, it means that the database synchronization has failed. Perform a manual Refresh Switch Data by following the steps below:

- 1) Navigate to Configuration > OpenScape Voice > General > Switches
- 2) Click Refresh Switch Data
- 3) After the refresh data is finished, double check the OS Voice Signaling protocol data again as described in the previous subchapter.
- 4) If the fields are still empty, then execute the following command in the backend node (with the system up and running):

```
/opt/siemens/assistant/scripts/cliSynchronization.sh  
user=administrator@system pw='Asd123!.' command=synchronize  
mode=osuc syncMode=full "
```

After executing this command, wait for a few minutes in order to have the SIP information in the table symDomain.symCommunicationSystems.

4.20.9 Extending the setup to internet usage

To extend the setup to the internet, use the TURN server from Media Server and the HAProxy.

4.20.9.1 Configuring TURN server from Media Server

It is recommended to use TURN in UDP configuration. However HA proxy does not support UDP, so it is necessary use an other port forwarder like for example SBC.

To use the WebRTC function with a multi Media Server system you need to route the TURN server related TCP/UDP traffic, based on destination port. Each TURN server listens to different port (HAProxy/SBC configuration).

NOTICE: It is possible to use more than one TURN options. For example: UDP, TCP and TLS.

Enable and configure the TURN server by editing the following file:

```
/opt/siemens/mediaserver/application_host/providers/turn/turn.component.xml
```

- 1) Set the realm to oscc.
- 2) Choose a password and set it on sharedSecret.
- 3) Set relay and transport addresses.
- 4) Set the path to the certificate and private key.

Sample Configuration:

```
<component name="turn"  
  class="com.cycos.media.turn.host.impl.TurnComponentImpl"  
  lazy="true">  
  <turnService>  
    <certificateFilePath>res/certificates/server.crt</  
certificateFilePath>
```



```

    <privateKeyFilePath>res/certificates/server.key</
privateKeyFilePath>
    <realm>oscc</realm>
    <sharedSecret>Test123!</sharedSecret>
    <relayAddresses>
    <address>192.168.159.51</address>
    </relayAddresses>
    <transportAddresses>
    <address>192.168.159.51:3478/UDP</address>
    <address>192.168.159.51:3478/TCP</address>
    <address>192.168.159.51:5349/TLS</address>
    </transportAddresses>
</turnService>
</component>

```

When IP addresses and/or ports are different from the defaults, they must be set on the transportAddresses block, e.g. "1.2.3.4:12345/TLS".

NOTICE: A detailed explanation of the configuration is available on the Media Server wiki: https://sdk.cycos.com/doku.php?id=dev:sdk:media_server:ivr:appendix:xmlfiles:mssettingsforturn9x

It is also possible to perform these configurations using the UI by following the steps below:

- 1) Navigate to Configuration > Unified Communication > Media Server > <webrtc_ms> > Providers > TURN (Traversal Using Relays around NAT)
- 2) Base Configuration

TURN (Traversal Using Relays around NAT) - Google Chrome

uc-vld-03-be.fusion6.net/management/portal/Applications/Operation/Configuration/mediaserver-mediaseverportlet/P...

TURN

Configure TURN services.

ID: 1 Add Remove

Base configuration Relay Addresses Peer Address Restrictions Transport Layer Security (TLS)

Realm: oscc

Shared secret: Test123!

Public address:

Deallocate on disconnect: ☐

IP differentiated services:

Service Addresses

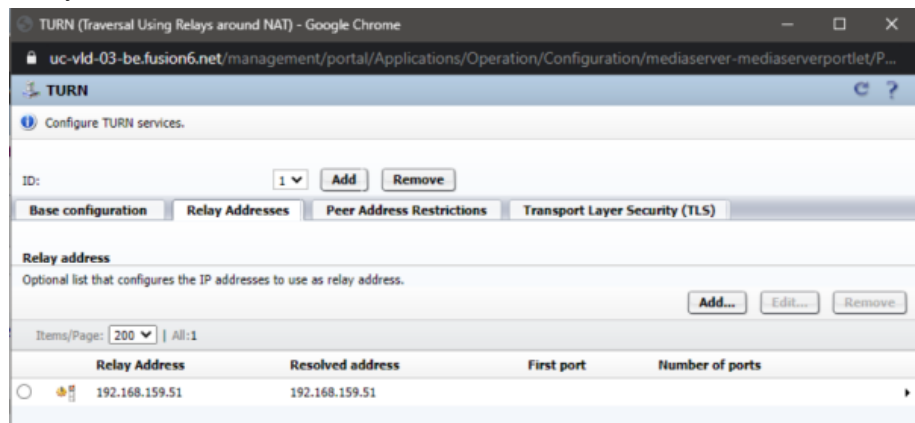
Optional list that configures the internet socket addresses to which a client could connect.

Add... Edit... Remove

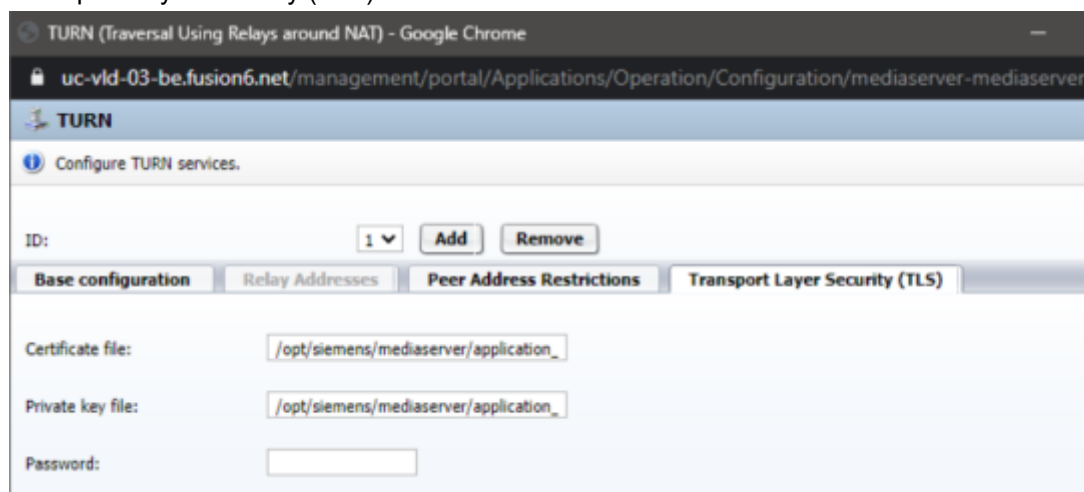
Items/Page: 200 All: 3

	Service address	Resolved address	Port number	First port	Number of ports	Transport protocol	Public address
☐	192.168.159.51	192.168.159.51	3478			UDP	
☐	192.168.159.51	192.168.159.51	3478			TCP	
☐	192.168.159.51	192.168.159.51	5349			TLS	

3) Relay Addresses



4) Transport Layer Security (TLS)



For the multiple Media Server usage of WebRTC, define the TURN URLs per Media Server node in the property TURNServerURLs of WebRTC MS Service in CMP.

4.20.9.2 Disabling ICMP error counting and Bandwidth adaptation within the streaming route of the MediaServer

When parameter icmpMonitoringEnabled is not set to false it may cause a call disconnection when starting streaming video using the TURN server.

When parameter rtpBandwidthAdaption and limitationMode is not set to OFF it may cause low quality in video calls.

- 1) Open the mfw.component.xml file and locate the path:

```
/opt/siemens/mediaserver/application_host/providers/streaming-mps/
mfw.component.xml
```

- 2) Change the parameter <rtpBandwidthAdaption mode="OFF"> to OFF and <limitationMode>OFF</limitationMode> to OFF and disable Bandwidth adaptation and Limitation Mode in the following way:

```
<rtpBandwidthAdaption mode="OFF">
  <!-- bandwidth adaption (resiliency) is enabled by
  default -->
```

```
<limitationMode>OFF</limitationMode>
</rtpBandwidthAdaption>
```

- 3) Change the parameter `<icmpMonitoringEnabled>>false</icmpMonitoringEnabled>` to false and disable ICMP monitoring of the appropriate streaming route in the following way:

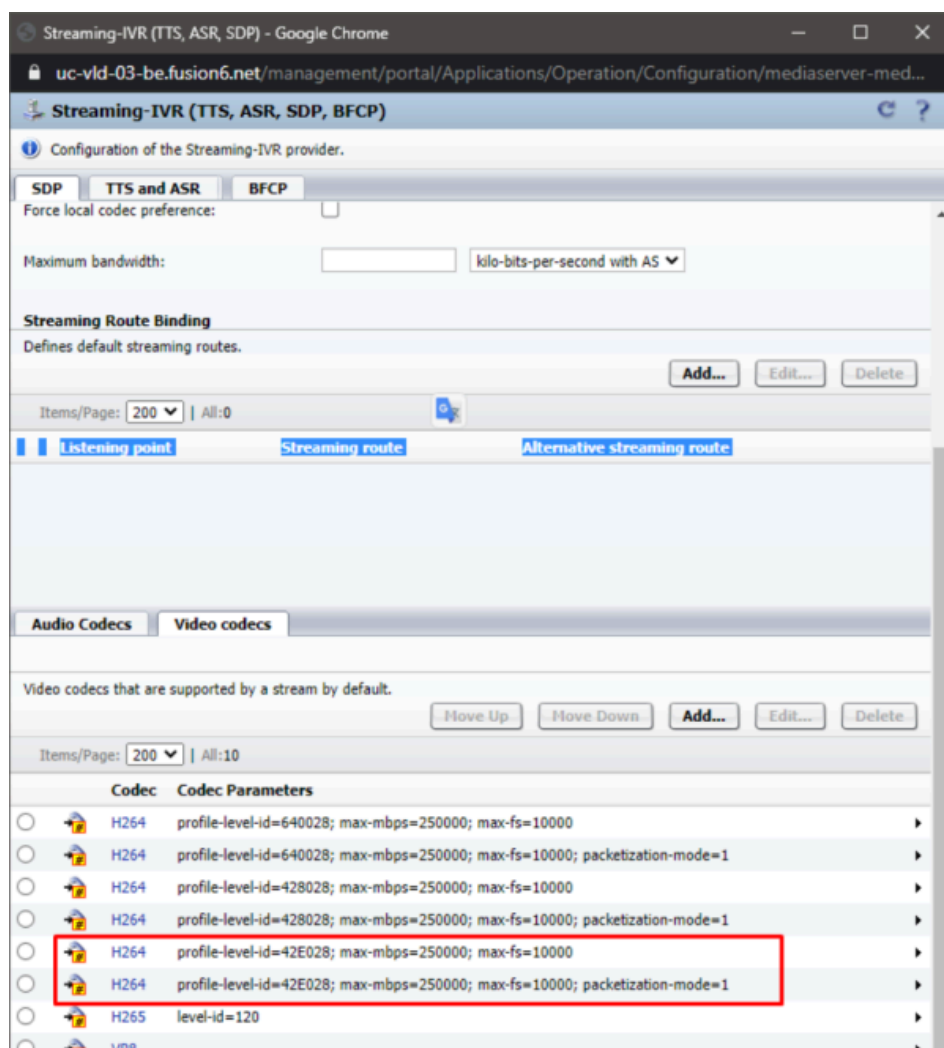
```
<mfwRoutesConfig>
  <streamingRoutes>
    <streamingRoute id="default">
      <icmpMonitoringEnabled>>false</icmpMonitoringEnabled>
      <icmpRecoveryTime>10</icmpRecoveryTime>
      <icmpUnreachableCount>200</icmpUnreachableCount>
      <ipAddress>auto$IPv4</ipAddress>
      <numRtpPorts>2500</numRtpPorts>
      <rtpPortRangeStart>20000</rtpPortRangeStart>
      <rtpTypeOfService>184</rtpTypeOfService>
      <rtpTypeOfServiceForVideo>136</
rtpTypeOfServiceForVideo>
    </streamingRoute>
  </streamingRoutes>
</mfwRoutesConfig>
```

- 4) Restart the media server services.

4.20.9.3 Video Codecs

Verify if the video codec 42E028 is created in Media Server video codecs. This is mandatory for WebRTC video calls.

Navigate to Configuration > Unified Communication > Media Server > <webrtc_ms> > Providers > Streaming-IVR (TTS, ASR, SDP, BFCP) > SDP > Video Codecs



4.20.9.4 Configuring the WebRTC Service

Follow the instructions below to configure the WebRTC Service:

- 1) Navigate to Maintenance > Inventory > Nodes > beservice > Show services status

2) Set the following parameters to:

a) TURNInfo TTL: 600 (Default)

b) TURNServerURIs:

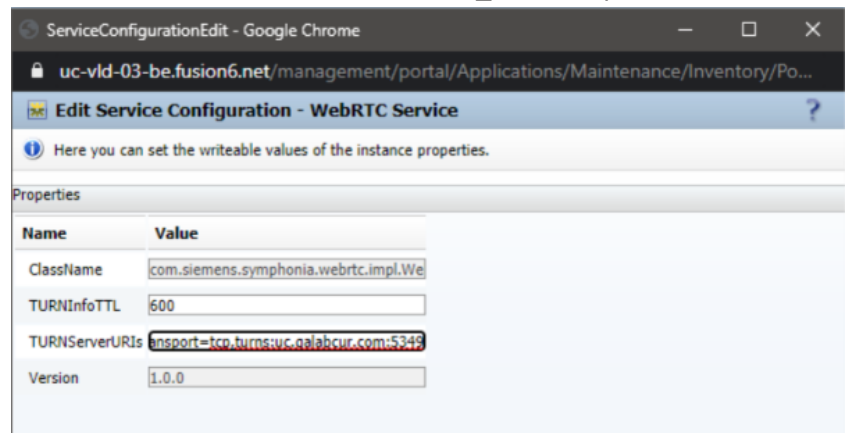
- To use UDP connection use:

turn:<turn_server>:<port>

- To use TCP connection use:

turn:<turn_server>:<port>?transport=tcp

- To use TLS connection use: turns:<turn_server>:<port>



4.20.9.5 Configuring WebRTC for a multiple Media Server system

To use multiple Media Servers of a WebRTC provider and to have these Media Servers accessible outside the corporate network you need to:

- Set a single public IP to expose all the Media Server nodes URLs along with the basic UC URL.
- Route your TURN server (related TCP/UDP traffic based on destination port). Please refer to [Configuring TURN server from Media Server](#) on page 316.
- Configure in CMP for each Media Server the following properties of WebRTC MS Service under Maintenance > Inventory > Nodes > Edit Service Configuration:

1) The TURN URL of the property TURNServerURIs

2) The external URL of the property MediaServerExternalURL

The MediaServerExternalURL property refers to the URL in which the specific Media Server can be accessed outside of the corporate network. Each one of the MS nodes will have a different URL.

For a “multiple MS system”, the “TURNServerURIs” field from the “WebRTC Service” settings (BE node) should be empty. Only the “TURNInfoTTL” field should be filled in.

Then, on each MS node, the “TURNServerURIs” field should be filled in (with the applicable URIs to that node), under the “WebRTC MS Service” settings.

When the “URI” syntax starts with “turn:” and the protocol is not specified, UDP is implied. Therefore, “turn:xx.xx:3478?transport=udp” can be simplified to “turn::xx.xx:3478”.

4.20.9.6 Configuring HAProxy

Configure the ports on HAProxy by editing the file:

`/usr/share/haproxy/ haproxy.cfg`

- HTTPS port for the WebClient (default is 8443).
- HTTPS port for the Media Server (default is 7443).
- TLS port for the TURN (default is 5349)

Sample Configuration:

```
global
#daemon
maxconn 150000
tune.ssl.default-dh-param 2048
defaults
mode http
timeout connect 5000ms
timeout client 120s
timeout server 120s
frontend FE-WebClient-VLD03
timeout client 120s
bind 192.168.158.81:8443 maxconn 65536 ssl crt /usr/share/haproxy/
default_haproxy_cert.pem
acl webkit path_beg -i /webkit
use_backend BE-MS-VLD03 if webkit
default_backend BE-WebClient-VLD03
frontend FE-TURN-VLD03_TLS
mode tcp
bind 192.168.158.81:5349 maxconn 65536 ssl crt /usr/share/haproxy/
default_haproxy_cert.pem
default_backend BE-TURN-VLD03
frontend FE-TURN-VLD03_TCP
mode tcp
bind 192.168.158.81:3478 maxconn 65536
default_backend BE-TURN-VLD03
backend BE-WebClient-VLD03
server WebClient-VLD03 192.168.159.50:8443 maxconn 150000 ssl verify none
backend BE-MS-VLD03
timeout server 120s
server MS-VLD03 192.168.159.51:7443 maxconn 150000 ssl verify none
backend BE-TURN-VLD03
```

```
mode tcp
```

```
server TURN-VLD03 192.168.159.51:5349 maxconn 150000 ssl verify none
```

NOTICE: When TLS is not used, remember to remove ssl configuration from haproxy.cfg.

NOTICE: Increase the default client and server timeout to "120s", or add "timeout client 120s" to the frontend block and "timeout server 120s" to the "mediaserver" backend block.

Multiple Media Server system:

Route the HTTP traffic to each Media Server node.

The HAProxy configuration uses one single port for the HTTP traffic (WebClient and WebRTC signaling), and two different ports for TURN. Please note that using one single TCP port for different services is only possible for HTTP traffic, since the "domain" part is a HTTP header.

You can find a "haproxy.cfg" sample here:

- WebClient access: <https://ucfe.domain.com:18443>
- External URL of MS1: <https://ms01.domain.com:18443/webkit>
- External URL of MS2: <https://ms02.domain.com:18443/webkit>
- TURN URI of MS1: turn:turn.domain.com:18478?transport=tcp
- TURN URI of MS2: turn:turn.domain.com:18479?transport=tcp
- "ms01.domain.com", "ms02.domain.com" and "turn.domain.com" resolve to the same public IP
- "1.2.3.4" is the HAProxy
- "192.168.0.2" is the FE
- "192.168.0.3" is the MS node 1

- “192.168.0.4” is the MS node 2

```
frontend https
mode http
acl is_ucfe hdr_dom(host) -i ucfe.domain.com
acl is_ms01 hdr_dom(host) -i ms01.domain.com
acl is_ms02 hdr_dom(host) -i ms02.domain.com
bind 1.2.3.4:18443 ssl crt /certificates/domain.com.pem
use_backend ucfe if is_ucfe
use_backend ms01 if is_ms01
use_backend ms02 if is_ms02
frontend turn
mode tcp
acl is_turn1 dst_port 18478
acl is_turn2 dst_port 18479
bind 1.2.3.4:18478
bind 1.2.3.4:18479
use_backend turn1 if is_turn1
use_backend turn2 if is_turn2
backend ucfe
option http-server-close
option http-keep-alive
server ucfe-node 192.168.0.2:8443 maxconn 5000 ssl verify none
backend ms01
option http-server-close
option http-keep-alive
server ms01-node 192.168.0.3:7443 maxconn 5000 ssl verify none
backend ms02
option http-server-close
option http-keep-alive
server ms02-node 192.168.0.4:7443 maxconn 5000 ssl verify none
backend turn1
mode tcp
server turn1-node 192.168.0.3:3478 maxconn 150000
backend turn2
mode tcp
server turn2-node 192.168.0.4:3478 maxconn 15000
```


Start the UC nodes:

The OpenScape UC server is ready to support WebRTC functionality. You can start UC node to get it up and running.

OpenScape UC Graph Connector

The OpenScape UC Graph Connector operates on the Facade node on port 10443 therefore, the connectivity between the external webhook listener url configured on port 8443 in the /graph/listen path must be proxied accordingly.

Sample configuration:

```
frontend FE-WebClient-VLD03
```

```
timeout client 120s
```

```
bind *:8443 maxconn 65536 ssl crt /usr/share/haproxy/
default _haproxy_cert.pem acl graph path_beg -i /graph/listen
```

```
#Enabled only if MS Graph Connector is enabled
```

```
use_backend graphconnector if graph
```

```
#MS Graph Connector on Facade node
```

```
backend graphconnector
```

```
server graphconnectorserver [Internal_IP_Facade_node]:10443 ssl verify none
```

NOTICE: The default certificate for the facade node must be replaced with a valid one signed by a Certificate Authority, otherwise the eventing webhook listener connectivity is not established by Microsoft Graph.

NOTICE: If you use the line `$(Enabled only WebClient is exposed over the internet)` you must add **!graph** after the **use_backend webclient_secure if secure !restricted1 !restricted2** line. Example: **use_backend webclient_secure if secure !restricted1 !restricted2 !graph** Alternatively, you can move the following line: `$(Enabled only if MS Graph Connector is enabled)` **use_backend graphconnector if graph** before the following line: `$(Enabled only WebClient is exposed over the internet)` **use_backend webclient_secure if secure !restricted1 !restricted2**

4.20.10 Configuring UC users

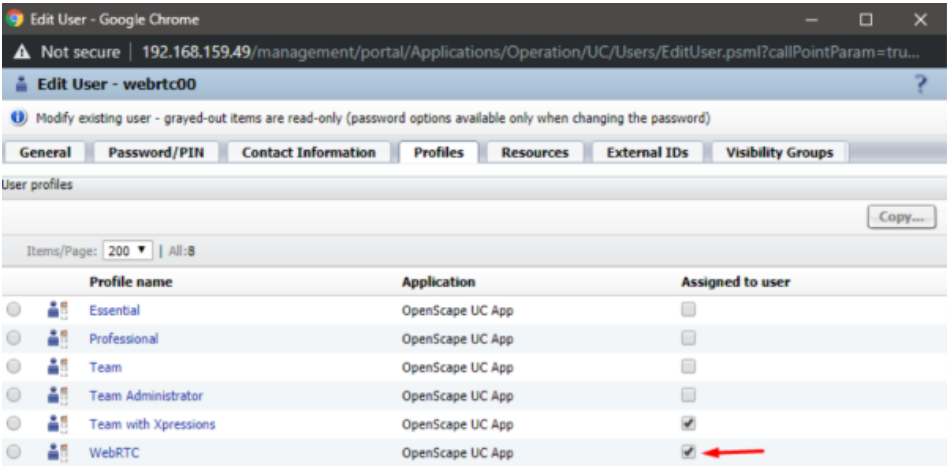
Define the users allowed to consume WebRTC licenses.

4.20.10.1 Configuring profiles

Assign WebRTC capability to the profile of the users allowed for this usage:

- 1) Navigate to Profiles > User profiles.

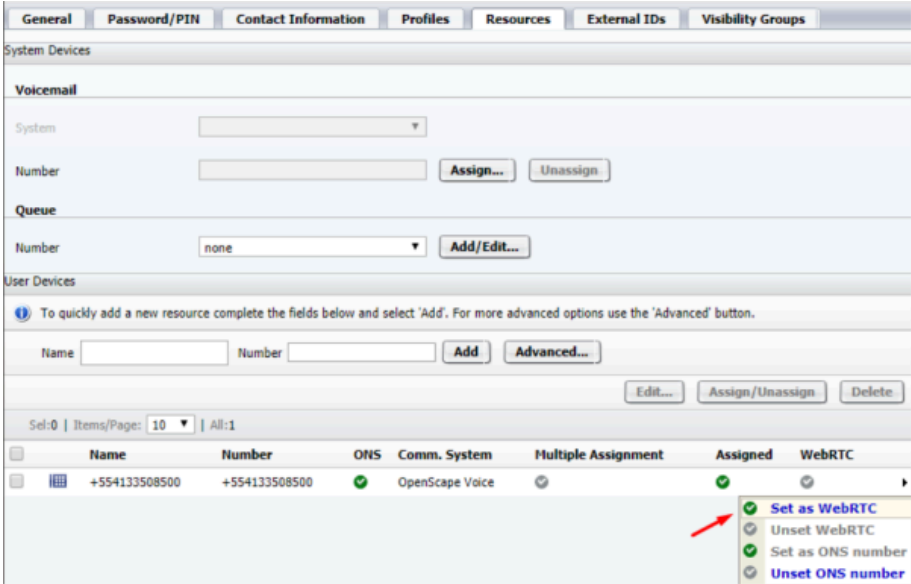
- 2) Check the Assigned to user option next to WebRTC as shown in the figure below:



4.20.10.2 Configuring devices (OND or ONS)

You must define which device will be assigned to control WebRTC activities for the user. It can be any OND or ONS device.

- 1) Navigate to Resources > User devices section.
- 2) Select the Set as WebRTC option from the drop-down list as shown in the figure below:



- 3) The new configured WebRTC device appears in the list with a green check indication under WebRTC as shown in the figure below:

The screenshot shows the 'Edit User' interface for user 'dida'. The 'User Devices' section contains a table with the following data:

	Name	Number	ONS	Comm. System	Multiple Assignment	Assigned	WebRTC
☐	+554133508850	+554133508850	✓	OpenScape Voice	✓	✓	✓
☐	+554133508504	+554133508504	✓	OpenScape Voice	✓	✓	✓

4.20.11 Configuring WebRTC Guest Access

4.20.11.1 Restrictions for WebRTC Guest Access

- Supported browser versions: only Google Chrome, Mozilla Firefox* and Microsoft Edge Chromium are supported by guest access feature.
- *Please check the Mozilla Firefox restriction for WebRTC Feature.
- Conference viewer link must be configured using https since WebRTC is not supported when http is used.
- A new attribute was added in WebRTC service configuration. The boolean attribute `GuestAccessEnabled` defines if the WebRTC guest access has been enabled or not (it is enabled by default).

Edit Service Configuration - WebRTC Service

Here you can set the writeable values of the instance properties.

Properties

Name	Value
ClassName	com.siemens.symphonia.webrtc.mpl.We
GuestAccessEnabled	true
TURNInfoTTL	665
TURNServerURIs	turn1.info.sm,turn2.info.sm
Version	3.0.0

Save

Cancel

- Regular expression for conference-default Address Binding is not supported for Guest Access:
 - Address Binding as "regexp:sip[+]554133508599.*" is not supported by Guest Access WebRTC feature.

It should be changed, or a new additional address binding should be added using single number e.g. "+554133508599" or a generic regular expression as "regexp:.+554133508599.*" should be used instead.

- You can find this configuration in the CMP:

Configuration > Unified Communications > Configuration > Media Server > Media Server Node > Address Binding

Node Administration - Google Chrome

uc-vld-03-be.fusion6.net/management/portal/Applications/Operation/Configuration/mediaserver-mediaseverportl...

Node administration

Administer the Media Server node 'uc-vld-03-ms'.

Providers Terminals **Address Binding** Applications Monitoring

Applied filter: Address=*, Application=*. This filter shows 17 out of 17 elements.

Edit filter ... Add ... Edit ... Delete

Items/Page: 200 | All: 17

	Address	Terminal ID	Application
☐	300	autoattendant-start	application:/Autoattendant#start
☐	301	autoattendant-startadmin	application:/Autoattendant#startAdmin
☐	notused	conferencing-callout	notused
☐	regexp:sip([+554133508599.*	conferencing-default	application:/Conferencing#welcome
☐	regexp:.+554133508599.*	conferencing-default-addnumbers	application:/Conferencing#welcome
☐	regexp:sip:933.*	conferencing-meetnow	application:/Conferencing#welcome_meetnow
☐	regexp:sip:983.*	conferencing-us	application:/Conferencing#welcome_us
☐	fastviewer:ary	Fastviewer	application:/Conferencing#fastviewer
☐	999	LocalParkSlot	application:/Transfer/CallIntoConference#IncomingCall
☐	mgcp:ann/*@*	Media Gateway - announcement endpoints	application:/MediaGateway#announcement
☐	mgcp:res/*@*	Media Gateway - CALIA/IS endpoints	application:/MediaGateway#res-conference
☐	mgcp:conf/*@*	Media Gateway - conference bridge endpoints	application:/MediaGateway#conference-bridge
☐	mgcp:ws/*@*	Media Gateway - whisper conference endpoints	application:/MediaGateway#whisper-conference
☐	101	voiceportal-guest	application:/Voiceportal#guest
☐	100	voiceportal-start	application:/Voiceportal#start
☐	201	voiceportal:speech-guest	application:/Voiceportal:speech#guest
☐	200	voiceportal:speech-start	application:/Voiceportal:speech#start

Close

System Configuration

- Guest WebRTC Access feature is limited to the "Number of joined participants determining suppression of join/leave indication".

NOTICE: If a conference was created with a number of participants higher or equal to this configured number, the Guest WebRTC Access will not work properly.

Media configuration - Google Chrome

uc-vid-03-be.fusion6.net/management/portal/Applications/Operation/UC/Configuration/symphonia-conferencingportl...

Media configuration

Audio settings Video Settings Video Performance Settings Web Collaboration

Default language
Set the default language for conferencing. Users who are unknown to the system hear the announcements in this language. For system users, the language set in the user settings applies.

English (United States) ▼

General settings
General settings for Telephone User Interface (TUI)

Play neutral welcome instead of branded one ☒

Short greeting when entering conference room (less prompts - only for audio devices) ☒

Fast transfer to conference room (no connecting prompts) ☒

Automatic Gain-Control - improved audio quality ☐

Play beep tone instead of longer join or left prompt (setting ignored when using name recording) ☒

Number of joined participants determining suppression of join/leave indication ←

Active speaker switch sensitivity
Speed of automatic switch-over to the active speaker.

Sensitivity level ▼

Save Cancel

NOTICE: This limitation is only valid for Open Conferences. For this reason, Moderated Conferences are recommended to use the guest access feature.

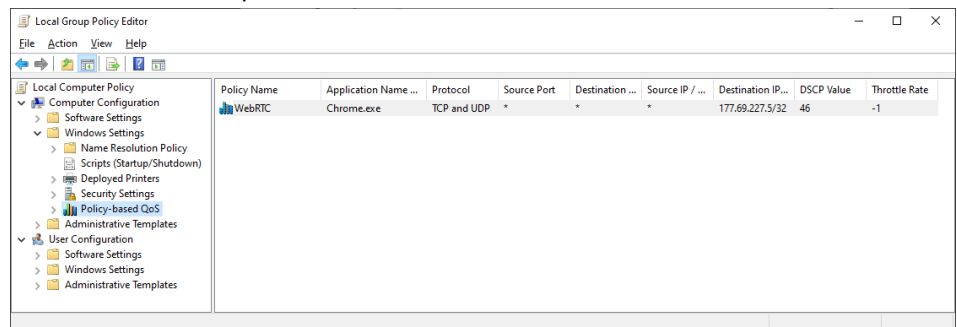
4.20.12 Configuring QoS

Quality of Service is typically implemented in VoIP networks to ensure optimal voice and video quality by prioritizing real time packets over less delay sensitive traffic. However, its use in WebRTC is not yet part of the standards, and not supported in browser implementations.

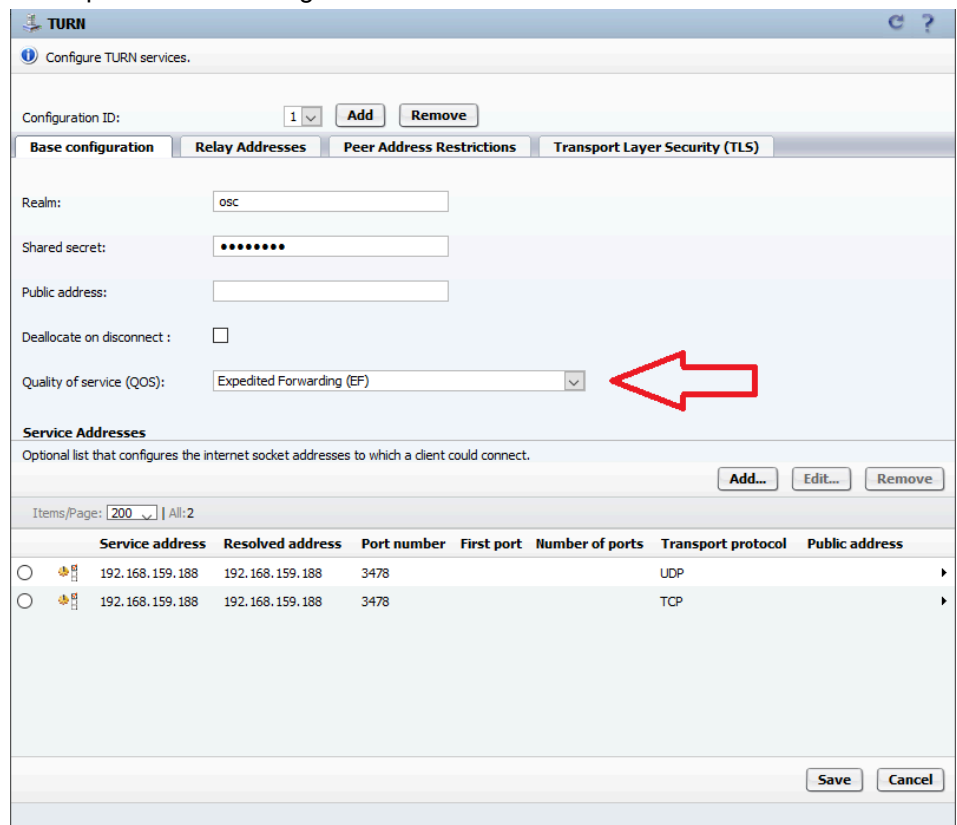
In addition, since the UC WebRTC solution is intended to be accessed over the open Internet, the benefits of QoS are limited to inside the LAN. That is because end-to-end QoS is not supported over the Internet. In particular, there is no guarantee that intermediate networks will honor DiffServ settings to give priority

to real time traffic. In fact, there is not even any guarantee that the DiffServ settings themselves will be transported unchanged.

The customer Network Administrator can use the Windows Group Policy Editor to centrally manage user PC QoS settings. For voice and video calls, it is recommended to use Expedited Forwarding (46). The GPE only allows policies to be based on source and destination IP/Port/Protocol. Therefore, it is not possible to differentiate between Voice and Video/Screensharing. It is only possible to differentiate realtime traffic from the signaling traffic as the latter uses a known TCP port.



On the TURN server side (Media Server node), it is also recommended to use the Expedited Forwarding value:



Bandwidth usage

Media type	Codec	Bandwidth
Audio	G.711, G.722	80 kbps

Media type	Codec	Bandwidth
Video	H.264	512 kbps
Screensharing	VP8	256 kbps

4.20.13 Configure WebRTC Screen Sharing

4.20.13.1 Prerequisites

- The OpenScape UC System must be configured for WebRTC and Guest Access features.

4.20.13.2 Configuration

The following parameter must be added in the file WebClientUI.cfg stored in the path of the UC backend:

```
/opt/siemens/HiPathCA/config/common
#
# 1. If set to true, this will enable WebRTC Screen
# Sharing (default value = false)
#
WebRTC.EnableScreenSharing = true
```

You should restart the OpenScape UC Server after this change.

To revert to FastViewer mode, change it back to false and restart the OpenScape UC Server.

NOTICE: Once the WebRTC Screen Sharing is activated, all new created conferences are video and screen sharing capable. There is no need to define this capability during the creation of the conferences.

WebRTC Screen Sharing for conferences created in previous releases before V11R2:

Conferences created without video prior to installation of V11R2 or above will have to be converted to video enabled to work with the WebRTC Screen Sharing.

The procedure is the following:

- 1) Install the Coman Tool as described in the Configuration and Administrator Documentation.
- 2) Export conference data using the following command:

```
C:\> java -jar coman.jar -s <osc-be-ip> -u <user-id> -p <user-
```



```
password> -e conferences.xls exportXLS
```

a) <osc-be-ip>:
The OSc Backend IP address.

b) <user-id>:
UserId of the domain user who wants to access the DB.

3) <user-password>:
The password of the domain user who is accessing DB.

4) Open conferences.xls.

a) Change values of the column "Video" from 0 to 1 to enable video (or from 1 to 0 to disable video).

b) Save the file conferences.xls.

5) Import new conference data using the following command:

```
C:\> java -jar coman.jar -s <osc-be-ip> -u <user-id> -p
<user-
password> -ow true -i conferences.xls
importXLS
```

The following command prints a help message to get more information about the Coman Tool

```
C:\> java -jar coman.jar -h
```

4.20.14 Hunt Group support in WebRTC softphone

The same hunt group functionality currently available for OpenScape Fusion is going to work with UC WebRTC softphones (Browser or UC Desktop App). See also chapter [Hunt Group Logon / Logoff](#).

You have to set the hunt group access codes in the WebClientUI.cfg file as follows:

```
#
# Multi Line Hunt Group - Busy address (e.g. *11)
#
MLHG.BusyAddress = *11
#
# Multi Line Hunt Group - Stop address (e.g. *12)
#
MLHG.StopAddress = *12
```

4.20.15 Configuring WebRTC Video resolution

The video resolution in WebRTC calls and conferences can be switched between VGA and HD (1280 x 720) using the WebRTC.EnableHDVideo parameter in the WebClientUI.cfg file.

- For VGA resolution (default) the parameter must be set to false.
"WebRTC.EnableHDVideo = false"

System Configuration

Enabling UC Desktop App download link

- For HD resolution the parameter must be set to true.

"WebRTC.EnableHDVideo = true"

In Video Conferences using the Common Video View Layout ([Common Video View Layout](#) on page 477), it is highly recommended to have all the connected clients working with the same video resolution. This optimizes the CPU load, reducing the number of video compositions in the UC server. If all Clients are using the same video resolution, there will be only one video composition in the UC server.

For HD Video settings (e.g. in Fusion Client), it is recommended to use 1024 (640 x 480) or 2048 (1280 x 720) as the network connection values of bandwidth, for both Download and Upload.

4.21 Enabling UC Desktop App download link

The UC WebClient has a Desktop Application version that you can use in your system. To use the UC Desktop App, you first need to enable the download link within the WebClient.

This can be configured by adding the UCDesktopDownload parameter in the WebClientUI.cfg file.

- 1) Navigate to:

/opt/siemens/HiPathCA/config/common/WebClientUI.cfg

- 2) In the WebClientUI.cfg file, set the value of the following parameter to true:

UCDesktopDownload = true

Now the Download UC Desktop Application link should be available in the WebClient from where you can download the Desktop App installation files..

4.22 Installing Keycloak

Keycloak is installed in the UC deployment BE server via the rpm package manager (keycloak-base rpm) that contains and also installs Java JDK 20.

The installation of Keycloak server and providers is performed automatically upon installation of UC. It includes a self signed certificate and starts in production mode.

The installation folder for Keycloak is the following:

/opt/siemens/share/keycloak/keycloak-21.1.1/data/import

Keycloak Admin URL

An example of the keycloak admin URL is: <https://ucdev31:8180/auth>, where ucdev31 is the hostname of BE node.

The default root credentials for the administrator console are the following:

- administrator
- Asd123!.

Keycloak configuration

To configure Keycloak, several manual steps are required:

Keycloak configuration files

- 1) Verify that `<keycloak_dir>/conf/keycloak.conf` and `<keycloak_dir>/data/import/uc-realm-export.json` are properly configured with the correct hostnames.

In `keycloak.conf`:

- `db-username` and `db-password` have the default MYSQL symphonia DB user respectively password set, but the customer can also use their own root credentials.
- `https-certificate-file` and `https-certificate-key-file` must contain the paths of the certificate and private key.

NOTICE: These files should be changed only if you use your own certificates.

- The `hostname` and `https-port` must contain the correct hostname and port that keycloak listens to.
- If HAProxy is available in the deployment, the following lines must be uncommented:

```
proxy=edge
hostname-port=<your_keycloak_port>
```

- 2) In the `uc-realm-export.json` file, verify the following parameters

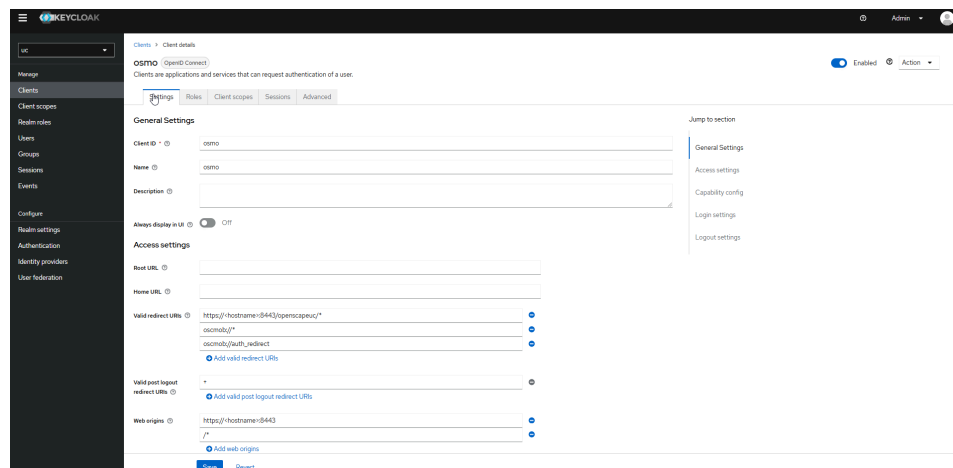
- `db-username` and `db-password` have the default MYSQL symphonia DB user respectively password set, but the customer can also use their own root credentials
- The UC FE/Load Balancer must be filled with either FE (`<hostname>:<port>`) or HAProxy (`<hostname>:<listener_port>`).

If you are using your own certificates, you must specify the paths (certificate / private key) in the `keycloak.conf` file and check that you have the correct hostnames and the fqdn of the backend where the keycloak server is installed.

Additionally, you must check that the following parameters are properly configured in the `uc-realm-export.json` file:

- `UC_BaseUrl` must include the hostname of BE
- UC FE/Load Balancer must include the `<hostname>:<port>` of either FE or HAProxy `<hostname>:<listener_port>`.

In **Keycloak admin**, the **osmo** client must be edited for a valid redirect URL. For this, `<hostname>` must be replaced with correct hostname.



Certificate Generation (automatic, by default)

Optionally, you can create your own self-signed certificate. This step is not mandatory and it is performed automatically.

Use the following command to create a self-signed certificate:

```
openssl req -x509 -sha256 -nodes -days 10000 -newkey  
rsa:2048 -keyout cert.key -out cert.crt
```

Next, you need to import the certificates (or a single rootCA):

- Keycloak (openjdk20) with Webclient FE certificate (or haproxy certificate)
- Webclient FE (ibm-jre 8) with keycloak certificate (or haproxy certificate)
- Keycloak (openjdk20) with mail server

To import a certificate in Java, you can use the commands below (example for IBM jre):

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -  
import -trustcacerts -keystore /opt/siemens/share/ibm-  
java-x86_64-80/jre/lib/security/cacerts -storepass  
changeit -noprompt -alias your_alias -file /path/to/  
your_certificate.crt
```

You can inspect the certificate using the following command:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -list  
-v -keystore /opt/siemens/share/ibm-java-x86_64-80/jre/lib/  
security/cacerts -storepass changeit -alias your_alias
```

Keycloak - SMTP Server configuration

After logging in to the Keycloak admin console (as root), follow the steps below:

- 1) Change the realm from "master" to "uc" (in the upper left part).
- 2) Navigate to Configure → Realm Settings → Email and add the SMTP server configuration.

Webclient configuration

The configuration file `/opt/siemens/HiPathCA/config/common/
WebClientUI.cfg` must contain the following:

```
# Support Two Factor Authentication (2FA) - Keycloak  
integration
```

```
# integration: If set to true, the WC will perform the user
authentication through the 3rd authentication server -
e.g. Keycloak (default value = false)
# url: Set the Keycloak server address and port, the WC
will be redirect to this address to proceed with the
login - Authentication provider address (default value =
[empty])
# realm: Set the realm configured at Keycloak for the
OpenScape integration. E.g.: uc - (mandatory field)
# clientid: Set the client ID configured at Keycloak for
the OpenScape integration. E.g.: osmo - (mandatory field)
#
keycloak.integration = true
keycloak.url = https://<hostname>:<port>
keycloak.realm = uc
keycloak.clientid = osmo
```

NOTICE: The realm and clientid fields are mandatory and must be filled with the values uc, respectively osmo.

To disable Keycloak, **keycloak.integration** must be set to false:

```
keycloak.integration = false
```

For the configuration changes to take effect, the BE node must be restarted using the following command:

```
systemctl restart symphoniad
```

You must check that the `WebClientServlet.cfg` file contains the correct information. This file is located in the following path:

```
/opt/siemens/HiPathCA/config/common/WebClientServlet.cfg
```

The example below shows a valid `WebClientServlet.cfg` file:

#Specify Keycloak information. Default value is empty

```
Keycloak.Host = facade.unify-dev.com
```

```
Keycloak.Port = 8444
```

```
Keycloak.Realm = uc
```

```
Keycloak.ClientId = osmo
```

```
Keycloak.ClientSecret =
```

You must ensure to provide the correct values for `Keycloak.Host` and `Keycloak.Port`.

- If the deployment includes a HAProxy, these parameters should have the hostname/port value of the HAProxy with the related listening port.
This is mandatory to be compliant with the OIDC protocol.
- If the deployment doesn't include an HAProxy, you simply need to provide the values for `Keycloak.Host` and `Keycloak.Port`.

The rest of the parameters should not be changed.

HAProxy configuration

An additional access control list must be added to resolve the `/auth` url path. Next, we need to redirect the request to the Keycloak server:

```
....  
acl keyclk path_beg -i /auth  
.....  
use_backend keycloak if keyclk  
...  
backend keycloak  
server keycloak  
server <BE_hostname>:8180 ssl verify none  
...
```

Additional information

- Useful commands for debugging Keycloak:

```
systemctl status/start/stop keycloak
```

```
journalctl -xef
```

```
/opt/siemens/share/keycloak/keycloak-21.1.1/bin/kc.sh  
show-config
```

When you make changes in the `keycloak.conf` file, it is recommended to build keycloak and start service.

```
/opt/siemens/share/keycloak/keycloak-21.1.1/bin/kc.sh  
build
```

- The users import is done automatically upon Keycloak installation.
- During the Keycloak installation, the 8180 default port is created. You can change the default port afterwards by editing the `keycloak.conf` file.

5 System Management for overlapping OpenScape Components

You find information about the following overlapping system management topics in the manual *OpenScape Common Management Platform, Administrator Documentation*.

- Managing system components
- Managing domains
- Managing user profiles
- Managing Licenses
- Importing and exporting System Data
- Backing up and restoring general OpenScape system components
- Managing the download center
- Managing the software repository
- Checking the system configuration consistency

6 System management for the components of OpenScape UC Application

This chapter provides information about how to manage the system components of OpenScape UC Application.

6.1 Dashboard for the System Nodes of OpenScape UC Application

For each OpenScape UC Application system node exist a dashboard that can be access via the CMP. This dashboard contains information on the corresponding system node. The information includes for example hardware information, alarm information, installed applications and their software level.

The following functions and information are available in the dashboard of a OpenScape UC Application system node.

- **Node Note**

By means of Edit you can add a individual note for the corresponding system node. In this way you are able to document information like the physical location of the node or the configuration of the corresponding computer system.

- **Alarm Summary**

Shows a summary of the alarms that are currently existing for the corresponding system node.

- **System Info**

Shows general information about the hardware of the corresponding system node. E. g.:

- CPU load
- Memory allocation

- **Applications**

Shows which applications of OpenScape UC Application are installed on the corresponding system node.

- **Actions**

By means of Show you are able to access the following information and functions of the corresponding system node.

- **UC Rapidstat**

You find detailed information about Rapidstat in the corresponding chapter.

- **Show service status**

Opens a dialog in which all components are shown that are installed on the corresponding system node for the available applications.

For each component is shown if it is started.

Furthermore you can configure settings for the individual components.

IMPORTANT:

Changing the component settings without appropriate knowledge may lead to wrong operation or no operation

at all for the relative application. Therefore, perform modifications only if the producer documentation or the producer's service personnel ask you to do so.

– **Show software packages**

Opens a dialog which shows all software packages that are installed on the corresponding system node with its individual software version.

6.2 UC User Administration

With the UC user management you administer the UC user accounts for the OpenScape system. This comprises in particular the user-individual contact information and access privileges.

Each UC user account specifies information about the following areas:

- General information
- Password/PIN
- Contact information
- Profiles
- Resources
- External IDs

These areas contain the following information:

General information

Information	Meaning
Login name	Specifies the user ID of the user account. The user deploys the user ID when logging on to the system. The following special characters must not be used for the user ID: ' - Apostrophe character @-character - Semicolon - Blank at the beginning or end of a login name
Domain	Default value is system
Display Name	Specifies the name displayed for the user account in the program's interface.
Home time zone	Specifies for the user account the date and time default format in the program interface of OpenScape UC Application.
Default language	Specifies the following for the user account: The language in which the OpenScape Web Client interface appears after the user has logged in. The language in which the voice portal plays greetings after the user identification.

Information	Meaning
Address Translation Context	You can choose from the available Address Translation Contexts or configure another Address Translation Contexts in the Configuration section of UC.
User locked	Locks the user account out of the OpenScape UC Application.

Password/PIN

Information	Meaning
Login password locked:	Shows whether the password-based access via the UC user account has automatically been locked. If the access is locked, the relevant user has entered an incorrect password too often while trying to log in.
Telephony PIN locked:	Shows whether the telephone-based access via the user account has automatically been locked. If the access is locked, the relevant user has entered an incorrect PIN too often while trying to log in.
Login Password	Specifies a new password for the user account. Passwords are assigned according to different policies that apply to the entire system.
Login Password never expires	Specifies that the password is infinitely valid. If the Password never expires and User has to change password at next login options are active at the same time, the relevant user needs to change his/her password at the next password-based login. The changed password is then infinitely valid.
User has to change login password at next login	Specifies that the relevant user needs to change the password at the next password-based login. This option is only valid until the next password-based login. After the login this option is disabled for the user account again. If the Password never expires and User has to change password at next login options are active at the same time, the relevant user needs to change his/her password at the next password-based login. The changed password is then infinitely valid.
New Telephony PIN	Specifies a new PIN for the user account.
Telephony PIN never expires	Specifies that the PIN is infinitely valid. If the PIN never expires and User has to change PIN at next login options are active at the same time, the relevant user needs to change his/her PIN at the next PIN-based login. The changed PIN is then infinitely valid.

Information	Meaning
User has to change telephony PIN at next login	Specifies that the relevant user needs to change the PIN at the next PIN-based login. This option is only valid until the next PIN-based login. After the login this option is disabled for the user account again. If the PIN never expires and User has to change PIN at next login options are active at the same time, the relevant user needs to change his/her PIN at the next PIN-based login. The changed PIN is then infinitely valid.

Contact information

Contains comprehensive contact information about the user of the user account.

Profiles

Lists all user profiles that are assigned to the user account.

Resources

Lists all resources that are assigned to the user account. These can be:

- Voicemail number

OpenScape UC Application uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called user. In this way no call is lost even if the called user cannot answer the phone. The voicemail number specifies the number of the called user's voicemail box.

- Queue number

NOTICE: This resource is not used by OpenScape UC Application

- User devices

Specifies the subscribers associated to the user. If you use OpenScape UC Application one of these subscribers can be set as ONS number.

External IDs

Lists all the External Identifiers of the UC User, e.g Groupware, Fusion, OpenScape Web Client Single Sign On etc.

NOTICE:

The External Identifier list will always contain the **contactSystem** which is the default external identifier that links contacts to users and cannot be modified.

In this section the Administrator has a Database view of a UC User's external identifiers so he/she can review the external identifiers and troubleshoot the configuration if needed.

Visibility Groups

This tab can be edited only after the new UC user is saved. In this section you can connect or disconnect a User to a Visibility Group.

6.2.1 How to Add a UC User Account

How to add a Unified Communications User Account:

Prerequisites

- Adequate administrative permissions

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.
A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Click on **Add**.
The dialog with the UC user account settings opens.
- 4) Specify the general settings for the new UC user account on the **General** tab.
- 5) Specify the password and PIN settings for the new user account on the **Password / PIN** tab.
- 6) Specify the contact data for the new user account on the **Contact Information** tab.

NOTICE: As soon as contact information is defined for a UC user account, a new contact is created in the integrated global contact list of OpenScape with this contact information.

The mandatory fields of the Contact Information tab are :

Last name

IM Address (in case there is no IM Address available you should enter the **Login name** value)

NOTICE:

E-mail Address 1 and **E-mail Address 2** fields' content are populated respectively in **Business e-mail** and **Home e-mail** fields of OpenScape Web Client, Mobile Client and OpenScape Mobile.

- 7) Activate the **Profiles** tab.

A list of all available UC Application and E/A cockpit profiles are displayed.

Click on the **Profile name** to see its permissions and possible licenses.

You can assign the desired user profiles to the new user account by checking the respective rectangular checkboxes in the **Assign to User** column or you can create a new profile by choosing one of the existing Profiles (check its radio button) and click on the Copy button.

- 8) Assign the desired resources to the new user account on the **Resources** tab.

You can configure resources that are assigned to the user account. These can be:

Voicemail number

OpenScape UC Application uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called user. In this way no call is lost even if the called user cannot answer the phone. The voicemail number specifies the number of the called user's voicemail box.

Queue number

Specifies the number of a multi-line hunt group used for the Ask-Me feature.

MLHG and PUG subscription codes

Specifies the MLHG and PUG subscription codes for a user. The configuration of this section is only enabled if you have set a resource as WebRTC.

You can manually enter values in the following fields:

- **Toggle MLHG Make Busy**
- **Toggle MLHG Stop Hunt**
- **Group Call Pickup**

NOTICE: It is not mandatory to enter a value for every field.

NOTICE: The validations that will be used are the same as we have in the Prefix Access Codes (Only digits and the characters #, *, +, A, B, C, D or E are allowed).

User devices

Specifies the subscribers associated to the user. If you use OpenScape UC Application one of these subscribers can be set as ONS and/or WebRTC number.

NOTICE: An External Resource can be re-used and assigned to more than one UC Users. Field **Multiple Assignment** informs about this.

- 9) **External IDs** tab can be edited only after the new UC user is saved.
- 10) **Visibility Groups** tab can be edited only after the new UC user is saved.
- The new UC user account is saved and displayed in the UC user accounts list.

NOTICE: It is not advisable to have more than one UC account that corresponds to one user. This option, although supported, needs extra caution when searching and adding users in a private contact list through OpenScape Web Client.

6.2.2 How to Edit a UC User Account's Settings

Prerequisites

- Adequate administrative permissions

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.
A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Click on the login name of the user account the settings of which you want to edit.
The dialog with the settings of the relevant UC user account opens.
- 4) Change the general settings for the relevant user account on the **General** tab.
- 5) Change the password and PIN settings for the relevant UC user account on the **Password / PIN** tab.
- 6) Change the contact data for the relevant UC user account on the **Contact Information** tab.

NOTICE: As soon as contact information is defined for a user account, a new contact is created in the integrated global contact list of OpenScape with this contact information.

The mandatory fields of the Contact Information tab are :

Last name

IM Address (in case there is no IM Address available you should enter the **Login name** value)

NOTICE:

E-mail Address 1 and **E-mail Address 2** fields' content are populated respectively in **Business e-mail** and **Home e-mail** fields of OpenScape Web Client, Mobile Client and OpenScape Mobile.

- 7) Change the UC user profile/ UC user account assignment on the **Profiles** tab.

NOTICE:

The **Foreign Profiles** tab shows all user profiles that are assigned to the user account in foreign-user domains.

- 8) Change the resources/user account assignment on the **Resources** tab.

You can configure resources that are assigned to the user account. These can be:

Voicemail number

OpenScape UC Application uses a workflow for incoming calls. This workflow always ends in the voicemail box of the called user. In this way no call is lost even if the called user cannot answer the phone. The voicemail number specifies the number of the called user's voicemail box.

Queue number

Specifies the number of a multi-line hunt group used for the Ask-Me feature.

MLHG and PUG subscription codes

Specifies the MLHG and PUG subscription codes for a user. The configuration of this section is only enabled if you have set a resource as WebRTC.

You can manually enter values in the following fields:

- **Toggle MLHG Make Busy**
- **Toggle MLHG Stop Hunt**
- **Group Call Pickup**

NOTICE: It is not mandatory to enter a value for every field.

NOTICE: The validations that will be used are the same as we have in the Prefix Access Codes (Only digits and the characters #, *, +, A, B, C, D or E are allowed).

User devices

Specifies the subscribers associated to the user. If you use OpenScape UC Application one of these subscribers can be set as ONS and/or WebRTC number.

- 9) Click on the **External IDs** tab to list all the External Identifiers of the UC User, e.g. Groupware, Fusion, OpenScape Web Client Single Sign On etc

IMPORTANT:

The External Identifier list will always contain the contactSystem which is the default external identifier that links contacts to users and cannot be modified or deleted.

Add a new External ID, configure any of the existing ones or delete one according to the " How to configure a UC User's External Identifiers " chapter

- 10) Click the Visibility Groups, to connect or disconnect a User to a Visibility Group.
- a) Select a Visibility Group from the list and click **Connect/Disconnect**.
 - b) Click **OK**.

- 11) Click on **Save** to copy the entries to the system's database.

6.2.3 How to Delete a UC User Account

Prerequisites

- Adequate administrative permissions

IMPORTANT: If the UC user to be deleted is also a E/A Cockpit member you must delete the E/A Cockpit member (or the entire E/A Cockpit) first.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.
A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Select the check boxes of the UC user accounts that you want to delete.
- 4) Click on **Delete**.
- 5) Click on **OK** to confirm the deletion of the selected user accounts.

The selected user accounts are removed from the system's database and from the list of all user accounts.

6.2.4 How to Display Bound Licenses of a UC User

With this task, it is possible to check the bound licenses assigned to a user. Users obtain licenses when they are assigned a profile containing the relevant features.

Prerequisites

- Adequate administrative permissions

Step by Step

- 1) Navigate to **Configuration > Unified Communications > Accounts > List**.
- 2) Select a User. Click on **Edit**.
The UC User window opens.
- 3) Click on the **Profiles** tab.
A list of the available Profiles appears.
- 4) Click on the **Show bound licenses** button.

The list of the user's bound licenses is displayed with the following information:

- **Product Name**
- **Feature Name**

6.2.5 How to Configure Existing Voicemail Numbers for a UC User Account

With this task, it is possible to check the bound licenses assigned to a user. Users obtain licenses when they are assigned a profile containing the relevant features.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.
A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Click on the login name of the desired UC user account.
The dialog with the settings of the relevant UC user account opens.
- 4) Click the **Resources** tab.
All resources assigned to the UC user account are displayed.
- 5) Click on the **Assign...** button in the **Voicemail** section.
A list of all phone numbers you can assign to the UC user account appears.
- 6) Select the check box of the phone number to which incoming calls are to be routed for the selected UC user account if required.
The selected phone number must be the access number of a voicemail system.
- 7) Click on **OK** to copy the selected phone number.
- 8) Click on **Save** to copy the entries to the system's database.

6.2.6 How to Configure Existing Voicemail Numbers for a UC User Account

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.
A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Click on the login name of the desired UC user account.
The dialog with the settings of the relevant UC user account opens.
- 4) Click the **Resources** tab.
All resources assigned to the UC user account are displayed.

- 5) Click on the **Assign...** button in the **Voicemail** section.

A list of all phone numbers you can assign to the UC user account appears.

- 6) Select the check box of the phone number to which incoming calls are to be routed for the selected UC user account if required.

The selected phone number must be the access number of a voicemail system.

- 7) Click on **OK** to copy the selected phone number.
- 8) Click on **Save** to copy the entries to the system's database.

6.2.7 How to Configure a New Voicemail Number for a UC User Account

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree, click on **Accounts > List**.

A list of all UC user accounts that are configured in the selected domain appears in the work area.

- 3) Click on the login name of the desired UC user account.

The dialog with the settings of the relevant UC user account opens.

- 4) Click the **Resources** tab.

All resources assigned to the UC user account are displayed.

- 5) Click on the **Assign...** button in the **Voicemail** section.

A list of all phone numbers you can assign to the UC user account appears.

- 6) Click on the **Add** button.

The dialog for creating a new voicemail number opens.

- 7) Enter under **Number** the phone number to which incoming calls are to be routed for the selected UC user account.

The phone number must be the access number of a voicemail system.

- 8) Click on **OK** to create the new phone number.

The new voicemail number is displayed in the list of phone numbers.

- 9) Select the check box of the newly created phone number.

- 10) Click on **OK** to copy the selected phone number.

- 11) Click on **Save** to copy the entries to the system's database.

6.2.8 How to Configure Subscriber Phone Number(s) for a UC User Account

You can assign one or several subscriber phone numbers to a UC user account, such as normalized numbers from the OpenScape Voice or an OpenScape

4000 connected to OpenScape UC Application (non-external resources), and additional phone numbers, such as mobile phone numbers (external resources). Assigning several subscriber phone numbers to a UC user account affects the following: The relevant UC user can choose one of the associated subscribers as preferred device in his/her OpenScape client. Furthermore, additional subscribers influence the media presence status of the relevant user if they belong to OpenScape Voice or a OpenScape 4000 connected to OpenScape UC Application.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

IMPORTANT: If there are multiple directory numbers belonging to a particular user, all these directory numbers must always be assigned to the corresponding UC user account.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree, click on **Accounts > List**.

A list of all UC user accounts that are configured in the selected domain appears in the work area.

- 3) Click on the login name of the desired UC user account.

The dialog with the settings of the relevant UC user account opens.

- 4) Click the **Resources** tab.

All resources assigned to the UC user account are displayed.

- 5) To add a new phone number from an external communication system (external resource):

- Under **User Devices**, enter the resource name in the **Name** field.
- Enter the resource number in the **Number** field (only numeric values are allowed).
- Click **Add**. The newly assigned phone number is now displayed as phone number entry under Number.
- Click **Save** to copy the entries to the system's database.

- 6) To add a new phone number from OpenScape Voice or OpenScape 4000 connected to OpenScape UC Application (non-external resource):

- Under **User Devices**, click **Advanced**.
- Check the box in front of the number you want to add.
- Click **OK**. The newly assigned phone number is now displayed as phone number entry under Number.
- Select **Set as ONS number**, to configure the phone number as ONS phone number. In the **ONS** column the phone number is indicated with  as ONS phone number.

IMPORTANT: The **Name** you configure for the ONS phone number will not appear in the UC clients, this

ONS number is always displayed with the name "office phone". The **Name** of the ONS phone number is also not contained in the domain export file.

- 7) To edit an assigned phone number:
 - Click the box in front of the resource you want to edit.
 - Click **Edit**. Alternatively, click the pointer button on the right of the resource and select **Edit**.
 - Edit the name of the resource in the **Name** field.
 - Click **OK**.
- 8) Click **Save** to copy the entries to the system's database.

6.2.9 How to Delete a Subscriber Phone Number(s) from a UC User Account

You can delete external phone numbers (external resources) and remove subscriber phone numbers of OpenScape Voice or OpenScape 4000 communication systems (non-external resources).

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.

A list of all UC user accounts that are configured in the selected domain appears in the work area.
- 3) Click on the login name of the required UC user account. Alternatively, click on the pointer icon on the right of the required user account and select **Edit**.

The dialog with the UC user account settings opens.
- 4) Click the **Resources** tab.

All resources assigned to the UC user account are displayed.
- 5) Delete an external phone number:
 - Check the box in front of the resource you want to delete.
 - Click **Delete**. Alternatively, click the pointer button on the right of the resource and select **Delete**.

The resource has been removed.
- 6) Delete an assigned non-external phone number (from OpenScape Voice or OpenScape 4000):
 - Click **Assign/Unassign**. Alternatively, click the pointer button on the right of the resource and select **Unassign**.
 - Click **OK**.
- 7) Click **Save** to copy the changes to the system's database.

6.2.10 How to Configure UC User's External Identifiers

Prerequisites

- Adequate administrative permissions.
- There is already a UC User configured.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Accounts > List**.

A list of all UC user accounts that are configured in the selected domain appears in the work area.

- 3) Click on the login name of the user account the External ID of which you want to configure.

The dialog with the settings of the relevant UC user account opens.

- 4) Click on the **External IDs** tab.
- 5) A Database View with a list of all the UC User's External IDs is displayed with the following database fields:

- **externalId**
- **assignedUserIdentity**

This is a read only value and is the fully qualified id of the UC User account.

- **assignedExternalSystemId.**
- **isContactMaster**
- **isProvisioningMaster**
- **additionalInfo**

These fields are populated when external systems are associated with the UC User (e.g. Groupware, Fusion, OpenScope Web Client Single Sign On etc.)

- 6) Click on the **Add** or **Edit** button to add a new or edit an existing External ID.

NOTICE: The External Identifier list will always contain the **contactSystem** which is the default external identifier that links contacts to users and cannot be modified or deleted.

The **Add External ID** or **Edit External ID** screen opens with the following fields:

externalId (mandatory field), **assignedUserIdentity** (mandatory field), **assignedExternalSystemId** (mandatory field), **ContactMaster**, **ProvisioningMaster**, **additionalInfo**

The Administrator can use these screens to review the external identifiers and troubleshoot the configuration if needed.

- 7) Click **Save** to copy the entries to the system's database.

6.2.11 How to Configure UC User Visibility Groups

How to add a Unified Communications User Account:

Prerequisites

- Adequate administrative permissions.

Step by Step

1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.

2) In the navigation tree, click on **Accounts > List**.

A list of all UC user accounts that are configured in the selected domain appears in the work area.

3) Select a user account and click on **Edit**.

The dialog with the UC user account settings opens.

4) Click the **Visibility Groups** tab. In this tab you can see the Visibility Groups that are connected.

a) To connect a new **Visibility Groups** click **Connect...** In this list you see only the Visibility Groups that are not yet connected to the UC User. Select one or more Visibility Groups from the list and click **OK**.

NOTICE: When adding a new UC user the **Connect** button is disabled. You first need to save the user in order to enable this button.

b) To disconnect a Visibility Group, select one or more from the list and click **Disconnect**.

5) Click **Save** to copy the entries to the system's database.

6.3 Team Configuration Overview

The **Team** feature allows every member of a team to pick up a call to the ONS device of every other colleague in the same team. You can configure the Team feature so the OpenScape User is allowed to set up his personal Team Contact List.

The following functions are supported for the Team Contact List:

- Team Configuration
- Access control
- Team view
- Call pickup in own team

Teams can be administrated by:

- The System Administrator
- UC Users with **Team Administrator** profile or with Group Management permissions enabled in their **OpenScape UC App** profile. These Team Administrators have the following buttons enabled in the OpenScape Web Client and subsequently the respective administration rights:
 - **Create team**

- **Delete team**
- **Add new member**
- **Delete member**
- **Assign/deassign a member as a team administrator**
- UC Users without **Team Administrator** profile and without the Group Management permission of their **OpenScape UC App** profile. These Team Administrators have the following limited set of buttons enabled in the OpenScape Web Client and subsequently the respective administration rights:
 - **Add new member**
 - **Delete member**
 - **Assign/deassign a member as a team administrator**

The System Administrator can manage all available teams in **CMP** or via Provisioning.

Team Administrators can only manage their own teams in the **OpenScape Web Client**.

Team Administrator

The System Administrator can define as a team Administrator any UC users of the Team.

Team administrators are team Administrators of the teams they create.

A team with members that don't have a team Administrator and can only be managed by the System Administrator.

The **Team Administrator** profile contains only one feature called *Symphonia Group Management*.

6.3.1 How to Display Unified Communication Teams

How to display the UC Teams:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Teams**.

A list of all **Unified Communication Teams** appears in the work area with the following info:

Name	Team Name
Administrator	List of Team Administrators . if there are no Administrators this field is empty

Description	Team Description

You can search with the Team **Name** or Team **Administrator** or Team **Member** values to filter the UC Team list.

NOTICE:

When you filter with **Member** option all teams including this member are displayed.

6.3.2 How to Add/Edit UC Teams

How to add/edit UC Teams:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Teams**.

A list of all **Unified Communication Teams** appears in the work area with the following info:

Name	Team Name
Administrator	List of Team Administrators . If there are no Administrators this field is empty
Description	Team Description

You can search with the Team **Name** or Team **Administrator** or Team **Member** values to filter the UC Team list.

- 3) Click on the **Add** button or choose one of the listed UC **Teams** and click **Edit**.

The dialog with the Team settings opens.

- 4) Navigate to the Information area and enter or modify the team's **Name** (mandatory) and **Description**.
- 5) Navigate to the Members area displaying a list of all UC Users that are members of this Team with the following information:

UC User Login Name	
UC User Name	If the Name is in bold fonts it indicates that this UC User is configured as a Team Administrator.

Team Status	Possible values: Forced Active: A member has been added to a team directly, i.e. without invitation, for example by a system administrator. The member is active. Accepted: A user that had been invited to the team by a team administrator and accepted the invitation. Removed: A member has been removed from a team but has not yet seen the notification about this. When the member has seen the notification, he can be finally deleted from the team. Declined: A user that had been invited to the team has declined the invitation. He can be re-invited by the team Administrator. Invited: A user has been invited to a team, e.g. added by a team Administrator, but has not yet accepted or declined the invitation.

- 6) Click on the **Set Team without Administrator** button if you don't want to have a team Administrator.

All team Administrators (names were in **bold**) are now just team members.

NOTICE:

The **Set Team without Administrator** button is active if a Team Administrator is assigned.

- 7) If you want to assign a Team member as a Team Administrator click on the action menu and choose the **Set as Administrator** option.

A team can have multiple **Team Administrators**.

You can set as Team Administrator any UC User of the Team. Depending on the UC User profile the Team Administrators will have two sets of administration rights in the OpenScape Web Client:

- If the Team Administrator has the **Team Administrator** profile or the **Group Management** permissions enabled in their **OpenScape UC App**

profile then the following OpenScape Web Client buttons are enabled for this administrator:

Create team

Delete team

Add new member

Delete member

Assign/deassign a member as a team administrator

- If the Team Administrator doesn't have the **Team Administrator** profile and the **Group Management** permissions is not enabled in their **OpenScape UC App** profile then only the following OpenScape Web Client buttons are enabled for this administrator:

Add new member

Delete member

Assign/deassign a member as a team administrator

NOTICE: If you remove the **Team Administrator** profile from a Team Administrator that doesn't have the **Group Management** permissions enabled in its **OpenScape UC App** profile then you will reduce the rights the Administrator has in OpenScape Web Client to the *limited* set.

- 8) Click on the **Add** button to add a UC User as a member to this Team.
- 9) Click on **Save** to copy the entries to the system's database.

Alternatively a System Administrator can use a CSV file which includes necessary object to create a team and add members to the team.

The System Administrator logs into **CMP** and navigates to **Maintenance > Recovery > Import** and imports the prepared CSV file.

The specified team with the specified members is created.

6.3.3 How to Delete a UC Team

How to delete a UC Team:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree, click on **Configuration > Teams**.

A list of all **Unified Communication Teams** appears in the work area with the following info:

Name	Team Name
Administrator	List of Team Administrators . If there are no Administrators this field is empty
Description	Team Description

You can search with the Team **Name** or Team **Administrator** values to filter the UC Team list.

- 3) Choose one of the listed UC **Teams** you want to remove and click on the **Delete** button.

The UC Team is deleted and the Team list is updated.

IMPORTANT: If an OpenScape UC User is deleted from the UC Accounts List then all Administrator privileges and memberships of this user in the teams will be canceled.

IMPORTANT: Alternatively a System Administrator can use a CSV file which includes necessary object to delete a team.

The System Administrator logs into **CMP** and navigates to **Maintenance > Recovery > Import** and imports the prepared CSV file.

The specified team is deleted.

6.3.4 How to Add a UC Team Member

How to add/edit a UC Team:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Teams**.

A list of all **Unified Communication Teams** appears in the work area with the following info:

Name	Team Name
Administrator	List of Team Administrators . If there are no Administrators this field is empty

Description	Team Description

You can search with the Team **Name** or Team **Administrator** values to filter the UC Team list.

- 3) Click on the **Add** button or choose one of the listed UC **Teams** and click **Edit**.

The dialog with the Team settings opens.

- 4) Navigate to the Information area and enter or modify the team's **Name** (mandatory) and **Description**.
- 5) Navigate to the Members area displaying a list of all UC Users that are members of this Team.
- 6) Click on the **Add** button to add a UC User as a member to this Team.

A list is displayed of all Unified Communications Users that have a profile of an *OpenScape UC Application* and are within the selected *domain*.

The list appears with the following information:

- **Login Name**
- **Name**
- **ONS**

You can search with the **Login Name** or **Name** values to filter the UC account list.

NOTICE: When adding a team member search is restricted to internal UC users only. External users from other UC clusters (e.g. on a very large deployment) cannot be members of the same team and they do not appear in the Directory search.

- 7) Choose the UC Users you want to add to the Team by ticking their respective checkbox.
- 8) Click on **OK** to copy the entries as Team Members.

NOTICE:

Alternatively a System Administrator can use a CSV file which includes necessary object to create a team and add members to the team.

The System Administrator logs into **CMP** and navigates to **Maintenance > Recovery > Import** and imports the prepared CSV file.

The specified team with the specified members is created.

6.3.5 How to Delete a UC User from a Team

How to delete a UC User from a UC Team:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.

- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigation tab, click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Teams**.

A list of all **Unified Communication Teams** appears in the work area with the following info:

Name	Team Name
Administrator	List of Team Administrators . If there are no Administrators this field is empty
Description	Team Description

You can search with the Team **Name** or Team **Administrator** values to filter the UC Team list.

- 3) Choose one of the listed UC **Teams** and click **Edit**.
The dialog with the Team settings opens.
- 4) Navigate to the Members area displaying a list of all UC Users that are members of this Team.
- 5) Choose the UC Users you want to delete from the Team by ticking their respective checkbox and click on the **Delete** button.

The UC users are deleted from the Team and the Member list of the Team is updated.

IMPORTANT: If an OpenScape UC User is deleted from the UC Accounts List then all Administrator privileges and memberships of this user in the teams will be cancelled.

NOTICE:

When the system administrator deletes a UC user from a team, the Team View of the deleted user as well as the Team View of the other team members do not display the change (deleted user) until the OpenScape Web Client page is manually refreshed or until the user logs-off from the OpenScape Web Client and logs-on again.

- 6) Click on **OK** to delete the entries from the Team Members.

IMPORTANT:

Alternatively a System Administrator can use a CSV file which includes necessary object to delete one or more team members from the Team.

The System Administrator logs into CMP and navigates to **Maintenance > Recovery > Import** and imports the prepared CSV file.

The specified members of the team are deleted.

6.3.6 How to Display Names in Journals of Team Members

Every member of a team can individually define for his or her call journal if it can be accessed by other team members. If this option is granted by a team member, the names of the call journal entries are by default replaced by question marks because of data privacy reasons. You may change this standard behaviour system-wide so that the corresponding names are displayed instead of the question marks.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.

Step by Step

- 1) Open the following configuration file in a text editor on the application computer of OpenScape UC Application.

```
config/services/default/JournalServlet/Jrn.cfg
```

- 2) Change the value for the following parameter from **NO** to **YES**.

ShowPersonalEntriesInPartnerJournal

- 3) Save the changed setting in the configuration file.
- 4) If you use a deployment scenario without front-end computer, execute the following command on the application computer to restart the web server component.

```
/etc/init.d/symphoniad restart WebClient
```

The web server component stops and immediately reboots again.

- 5) If you use a deployment scenario with front-end computer, proceed as follows to reboot the web server component.
 - a) Execute the following command on every front-end computer to restart the relevant web server component.

```
/etc/init.d/symphoniad restart WebClient_FE
```

The relevant web server component stops and immediately reboots again. All settings performed so far become effective on the relevant front-end computer.

- b) Execute the following command on the application computer to restart the relevant web server component.

```
/etc/init.d/symphoniad restart WebClient_BE
```

For the call journal entries of other team members also the corresponding names are displayed.

6.3.7 How to modify the Team Toaster delay pop up notification

With V9R3 you can configure the **Team Toaster delay pop up notification**.

In case you want to answer a call for a team member via the Team Toaster pop up, the delay of the Team Toaster pop up notification can be configured.

In order to configure this delay of the pop up notification edit file <Osc - Install>/HipPathCA/config/services/default/GroupService/GroupService.c

NOTICE: p

NOTICE:

<Osc-Install> is the setup directory of OpenScape UC Application:

/opt/siemens/ respectively /enterprise/

Modify the parameter **groupcall.delay**.

groupcall.delay = 5000

The default value is 5000 ms.

Setting this parameter to 0 means no delay.

6.4 Visibility Groups Configuration Overview

UC software allows the use of multiple directory connectors for contact searches. This feature, i.e Visibility Groups, offers selective access to LDAP connectors on a per user basis. Connections can be set up to different LDAP servers. However, multiple different connections can also be set up to the same LDAP server.

6.4.1 How to Add/Edit a Visibility Group

Follow the steps below to add/edit a Unified Communication Visibility Group:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the CMP and navigate to the **Configuration > Unified Communications** tab.
- 2) In the navigation tree, click on **Visibility Groups** in the Configuration section.

A window opens that displays the Unified Communications Visibility Groups.

- 3) Click **Add**.

The dialog window **Add Visibility Group** opens.

- 4) Specify the **Name** property by typing a name under which the Visibility Group is to be displayed.

NOTICE: The **Name** field is mandatory for the Visibility Group and cannot be left blank.

- 5) Enter a description for your Visibility Group in the **Description** section (optional).

- 6) Select a value from the drop down menu **LDAP Connector** to choose the LDAP connector that you want to connect to this Visibility Group. An LDAP connector option consists of two parts:

The first part is the display name of the LDAP connector, which can be configured under **Configuration > Unified Communications > Connections > LDAP**.

The second part is the id of the connector which is actually the way it is saved and is automatically configured.

NOTICE: You will not be able to select a LDAP Connector used by an other Visibility Group because they have one to one relationship

- 7) Click **Save** to add the Visibility Group.

The dialog window will close and you will be able to see the new Visibility Group in the initial window.

- 8) Click on the Visibility Group you have created, and click **Edit**.

6.4.2 How to Delete a UC Visibility Group

Follow the steps below to delete a Unified Communication Visibility Group:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the CMP and navigate to the **Configuration > Unified Communications** tab.
- 2) In the navigation tree, click on **Visibility Groups** in the Configuration section.

A list of the Unified Communications Visibility Groups appears.
- 3) Select the Visibility Group you want to delete and click **Delete**.
- 4) Click **OK**.

6.4.3 How to Assign Visibility Groups Feature to an Administrator

You can assign Visibility Groups feature by following the steps below:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the CMP and navigate to the **Configuration > CMP** tab.
- 2) In the navigation tree, click on **Profiles** in the General section.

3) Click **Add**.

The dialog window **Add Profile** opens.

4) Check or uncheck the option Visibility Groups to assign or unassign the Visibility Groups feature.

6.5 Contact List Management

Using the contact list management you administer the different contact lists of the OpenScape system.

NOTICE: The contact list management is only required if you use OpenScape UC Application.

IMPORTANT: The optional Facade server caches the directory configured as global or private contact list in its local cache. This cache is not automatically updated if another directory is configured as private or global contact list. Therefore, you need to manually reboot the optional Facade server for another contact list to take effect.

The OpenScape system provides different contact lists. We can generally distinguish two types.

- Global contact lists
- Private contact lists

Global Contact List

Global contact lists contain the global contact data of users. For example, the contact data of a company's employees. OpenScape UC Application currently supports as global contact lists:

- The integrated global contact list of OpenScape UC Application.

NOTICE: As soon as contact information is defined for a UC user account or a CMP Administration user account in Common Management Platform , a new contact is created in the integrated global contact list of OpenScape UC Application with this contact information.

NOTICE: The new contact of the UC user can be deleted or unlinked if it is not assigned to a UM user. The new contact of the CMP administrator account can't be deleted or unlinked.

- An external LDAP directory that is connected to OpenScape UC Application via the LDAP connector.

You can use the contact list management to do the following:

- Define, which of these global contact lists should be used. In these active contact lists the OpenScape applications can then look for contact information.

- Manage contacts in the global contact list that is integrated in OpenScape UC Application.

NOTICE: OpenScape UC Application has only read-access to the contacts of a connected LDAP directory.

Private Contact List

Private contact lists contain contact data that single users maintain for their own use. Such data can only be created and edited by the respective user and via the OpenScape applications.

You can use the contact list management to define where the private contact list of the various OpenScape users shall be managed. For the time being, this can be one of the following places:

- The integrated OpenScape UC Application contact database.
- A groupware system connected to OpenScape UC Application via the groupware connector.

The OpenScape applications use certain services to access the contact lists. To this, the services need to register with the OpenScape system beforehand. In certain circumstances, a service may be configured, but not registered, in which case it cannot be accessed.

6.5.1 How to Display list of Global Contact

How to display the Global Contact List:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Contacts**.

The work area displays a list of all contacts that are available in the global contact list of OpenScape UC Application with the following information:

- **Last name** of the Contact
- **First name** of the Contact
- **Link to user:** Displays the User linked to the Contact
- **Business Phone 1** of the Contact
- **E-mail** of the Contact

6.5.2 How to Add a Global Contact

How to add a Global Contact:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: You have only read-access to the contacts of a connected LDAP directory.

Step by Step

- 1) Log in to the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree, click on **Contacts**.

The work area displays a list of all contacts that are available in the global contact list of OpenScape UC Application.

- 3) Click on **Add**.

The dialog with the global-contact information opens.

- 4) Enter the desired contact information on the **Phone & Contact** tab.

NOTICE:

The **Sound like** field must have an entry that will help an ASR (automatic speech recognition) to recognize the spoken name of the user.

- 5) Enter the desired address information on the **Address & Location** tab.

- 6) The **System** tab fields are read only and have Internal Information.

- 7) In the **Custom Fields** tab you can enter up to six **Client Matter Codes** and their relative **Custom Fields**.

CMC (**Client Matter Codes**) is used for accounting and billing purposes.

Client Matter Codes force the user (when making a call) to enter a code to specify that the call relates to a specific client matter.

The **Custom Fields** are used to store arbitrary data regarding the Client Matter Codes.

- 8) Click on **Save** to copy the entries to the system's database.

The new contact is displayed in the list of all global contacts.

Next steps

After you create a Global contact you can link it to a UC user:

- Navigate to **Configuration > Unified Communications > Contacts** choose the new Global Contact and click on the action menu.
- Click on the **Link to User** option.

- The list of users appear and you can select the by clicking on the relative radio button of the user you want to connect to the Contact.
If you select a user that is already linked to a contact an error message appears.
- Click on **Select**.

6.5.3 How to Edit a Global Contact

How to edit a Global Contact:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: You have only read-access to the contacts of a connected LDAP directory.

Step by Step

- 1) Log in to the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Contacts**.
The work area displays a list of all contacts that are available in the global contact list of OpenScape UC Application.
- 3) Click on the last name of the desired contact.
The dialog with the settings of the relevant contact opens.
- 4) Enter the desired contact information on the **Phone & Contact** tab.

NOTICE:

The **Sound like** field must have an entry that will help an ASR (automatic speech recognition) to recognize the spoken name of the user.

- 5) Enter the desired address information on the **Address & Location** tab.
- 6) The **System** tab fields are read only and have Internal Information.
- 7) In the **Custom Fields** tab you can enter up to six **Client Matter Codes** and their relative **Custom Fields**.

CMC (**Client Matter Codes**) is used for accounting and billing purposes.

Client Matter Codes force the user (when making a call) to enter a code to specify that the call relates to a specific client matter.

The **Custom Fields** are used to store arbitrary data regarding the **Client Matter Codes**.

Next steps

A Global Contact can be unlinked from the user:

- Navigate to **Configuration > Unified Communications > Contacts** choose the Global Contact you want to Unlink and click on the action menu.

- Click on the **Unlink from User** option.

The contact will be unlinked as long as the user isn't a UM user or an Administrator.

A Global Contact can be linked to a UC user:

- Navigate to **Configuration > Unified Communications > Contacts** choose the Global Contact you want to link to a user and click on the action menu.
- Click on the **Link from User** option.
- The list of users appear and you can select the by clicking on the relative radio button of the user you want to connect to the Contact.

If you select a user that is already linked to a contact an error message appears.

- Click on **Select**.

6.5.4 How to Link a Global Contact to a UC User

How to link a Global Contact to a UC User:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Contacts**.

The work area displays a list of all contacts that are available in the global contact list of OpenScape UC Application.

- 3) Click on the action menu of the Global Contact you wish to link to a UC User.
- 4) Click on the **Link to User** option.

The list of UC users appear and you can select the user you want to connect to the Contact by clicking on the relative radio button.

- 5) Click on **Select**.

NOTICE:

If you select a user that is already linked to a contact an error message appears.

6.5.5 How to Link a Global Contact to a UC User

How to display Available Contact Lists:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) Log in to the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click:
 - **Contact Settings > Global List** to display the available global contact lists.
 - **Contact Settings > Private List** to display the available private contact lists.

6.5.6 How to Define the Global Contact List as Active Contact List

How to define a Global Contact List as Active Contact List:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Contact Settings > Global List**.

A list of all global contact lists available in the OpenScape system is displayed in the work area.
- 3) Select the check boxes of the contact lists to be used as active contact lists.
- 4) Click on **Save current selection** to copy the entries to the system's database.

NOTICE: If the OSUC Client is to show the presence status of a locally added contact, the related **IM address** must be defined in the corresponding contact data. This is ensured if the contact was added to the OSUC Client's local contacts via the global contact list while the **GlobalContactList-Service** was configured as global contact list.

6.5.7 How to Cancel the Status of an Active Global Contact List

How to Cancel the Status of an Active Global Contact List:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree click, click on **Contact Settings > Global List**.

A list of all global contact lists available in the OpenScape system is displayed in the work area.

- 3) Deactivate the check boxes of the contact lists no longer to be used as active contact lists.



WARNING: It is not supported to deactivate the **GlobalContactList-Service** in a regular OpenScape UC installation.

- 4) Click on **Save current selection** to copy the entries to the system's database.

6.5.8 How to Specify a Storage Location for Private Contact Lists

How to Specify a Storage Location for Private Contact Lists:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Contact Settings > Private List**.
A list of all private contact lists available in the OpenScape system is displayed in the work area.
- 3) Select the check box of the contact list in which the private contact list of the various OpenScape users is to be managed.
- 4) Click on **Set Default Contact Lists**.

6.6 Communication System Resources

The Devices group contains resources available for all communications system in the Common Management Platform. The resources of this group are configured in the relative Communication System. They can therefore only be edited via the resource management of the Common Management Platform. The resources of these Communication Systems can only be added or deleted within the relative Communication System.

The Common Management Platform administers the following resources with the described settings.

- **Office Codes**

An office code represents the general portions of a phone number that precedes the extension number. These are:

Country code – Area code – Local Office Code for Public Numbering Plan

and respectively

L2 code - L1 code - L0 Code for a Private Numbering Plan

Example: 0049 - 89 - 722

In case of an OpenScape Voice Communication system the office codes are configured with the OpenScape Voice Assistant.

An office code may contain a so-called **overlap**. This overlap specifies if and to what extent the office code and the associated extensions overlap.

Example: A fully qualified phone number be 492404902100. The office code is 492404902 and the extension 2100. In this example, one digit of the extension and office code overlap – namely digit 2. The **overlap** in this example is thus 1.

In case of a Public Numbering Plan the **overlap** field can be configured with a negative value so in the example above:

- if the **overlap** is 0 the extension =100
- if the **overlap** is -2 the extension = 0

NOTICE: Private Numbering Plans can't have negative **overlap** values.

If an office code is to use an **overlap**, it must be configured via the resource management of the Common Management Platform.

An office code is fully configured from the OpenScape UC Application view, if the **overlap** field is configured.

Whether or not an office code is fully configured it is depicted in the **Complete** column with a green or grey color.

IMPORTANT: OpenScape 4000 Communication Systems with private Office Codes and public Prefixes or vice versa can't be synchronized and therefore not supported when adding a OpenScape 4000 node.

NOTICE: Unknown office codes of the OpenScape 4000 Communication System are displayed with their Node Access Code.

- **Prefixes**

Depending on the dialling plan (private or public) the prefix is configured with the following attributes:

Private	Public
L2 Prefix	International Prefix

L2 Network Access Code	International Network Access Code
L1 Prefix	National Prefix
L1 Network Access Code	National Network Access Code
L0 Prefix	Subscriber Prefix
L0 Network Access Code	Subscriber Network Access Code

- **Voice Subscribers**
- **Conference Devices**

A conference device of the OpenScape Media Server corresponds to the phone number for an OpenScape Voice or OpenScape 4000 system.

It defines a public or private extension that is assigned to an office code and a prefix.

The conference type specifies whether the device is associated to the conference portal or the voice portal of the OpenScape Media Server.

6.6.1 How to Display Office Codes

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a communication system can only be modified in the CMP.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Offline Codes**.
- 3) In the workspace select the Communication System from the drop down menu **Comm. System**.

A list of all Office Codes configured in the selected communication system appears in the work area.

- 4) Following attributes of the Office Code are displayed in the workspace:

Attribute	Sorting available
Office Code / Node Access Code	yes
Type	yes
Overlap	no
Complete	yes

6.6.2 How to Edit Office Codes

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a communication system can only be modified in the CMP.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Offline Codes**.
- 3) In the workspace select the Communication System from the drop down menu **Comm. System**.

A list of all Office Codes configured in the selected communication system appears in the work area.

- 4) Following attributes of the Office Code are displayed in the workspace:

Attribute	Sorting available
Office Code / Node Access Code	yes
Type	yes
Overlap	no
Complete	yes

- 5) Tick the checkbox of the office code you wish to edit and click on **Edit**.

The dialog with the office code settings opens.

6) Change the resource settings making sure you follow the conditions below:

- a) If you are editing a Public Office Code you can only modify the **overlap** field and the value can't be larger than the number of the Local Office Code digits. You can also enter a negative value in the **overlap** field.

Example : If a fully qualified phone number is 492404902100 and the office code is 492404902

if the **overlap** is 1 the extension =2100

if the **overlap** is 0 the extension =100

if the **overlap** is -1 the extension =00

if the **overlap** is -2 the extension = 0

- b) If you are editing a **Private Office Code** you can only shift digits between the L0,L1 and L2 code so the full code will not change and making sure L0 code is never null.

The **overlap** value can't be larger than the number of the L0 Code digits and can't have a negative value.

- c) Additionally if you are editing a Private Office Code and a L2 Code is set then L1 Code field must not be empty.

7) Click on **Save** to copy the entries to the system's database.

Changing the values of an office code which is marked as completed will require a manual restart of the UC server and will also trigger the relevant Major Alarm.

6.6.3 How to Display Prefixes

All prefixes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Prefixes of a communication system can only be modified in the CMP.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Offline Codes**.
- 3) In the workspace select the Communication System from the drop down menu **Comm. System**.

A list of all Prefixes configured in the selected communication system appears in the work area.

- 4) Following attributes of the Prefixes are displayed in the workspace depending on the Prefix Type (Private or Public).

Private	Sorting available
L2 Prefix	International Prefix
L2 Network Access Code	International Network Access Code
L1 Prefix	National Prefix
L1 Network Access Code	National Network Access Code
L0 Prefix	Subscriber Prefix
L0 Network Access Code	Subscriber Network Access Code

6.6.4 How to Edit Prefixes

All prefixes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Prefixes of a communication system in the CMP can only be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Offline Codes**.
- 3) In the workspace select the Communication System from the drop down menu **Comm. System**.

A list of all Prefixes configured in the selected communication system appears in the work area.

- 4) Tick the checkbox of the prefix you wish to edit and click on **Edit**.

The dialog with the prefix settings opens and depending on the Prefix Type (Private or Public) following attributes can be edited.

Prefix Id	Prefix Id
Type Private	Type Public
L2 Prefix	International Prefix
L2 Network Access Code	International Network Access Code
L1 Prefix	National Prefix

L1 Network Access Code	National Network Access Code
L0 Prefix	Subscriber Prefix
L0 Network Access Code	Subscriber Network Access Code
Complete	Complete

NOTICE:

An "incomplete" prefix of a communication system will be set to "complete" as soon as it is manually updated for the first time, even if no values are set or modified for the first time.

- 5) Change the resource settings.
- 6) Click on **Save** to copy the entries to the system's database.

6.6.5 How to Display Voice Subscribers

All Voice Subscribers of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: The Voice Subscribers of a communication system in the CMP can only be edited.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Voice Subscribers**.
- 3) If you wish to display a Voice Subscriber or a list of Voice Subscribers, specify in the display filter a search criterion that the desired resource matches and click on **Search**.

NOTICE: You can display all voice subscribers that belong to all communications systems within a domain.

IMPORTANT: If you haven't selected a Communication System in your search filter then no Subscriber is displayed and following message appears in information

area: To search for voice subscribers you must select a Communication System from the drop-down menu

The list of all subscribers that match the search criterion will be displayed with the following attributes:

Attribute	Sorting available	Description
Normalized Number	yes	
Public Extension	yes	digits displayed depend on the overlap value defined in the office code configuration
Private Extension	yes	digits displayed depend on the overlap value defined in the office code configuration
BC Federation	no	
Comm. System	no	column appears only when All comm. Systems are in display
Unique	no	Unique numbers are the ones that belong to non VNR OpenScape 4000 switches
ONS	no	yes or no
Virtual Node ID	no	Virtual Node IDs are applicable only to VNR OpenScape 4000 switches

6.6.6 How to Edit Voice Subscribers

All Voice Subscribers of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: The Voice Subscribers of a communication system in the CMP can only be edited.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Voice Subscribers**.

- 3) If you wish to display a Voice Subscriber or a list of Voice Subscribers, specify in the display filter a search criterion that the desired resource matches and click on **Search**.

IMPORTANT: If you haven't selected a Communication System in your search filter then no Subscriber is displayed and following message appears in information area: *To search for voice subscribers you must select a Communication System from the drop-down menu*

The list of all subscribers that match the search criterion will be displayed with the following attributes:

Attribute	Sorting available	Description
Normalized Number	yes	
Public Extension	yes	digits displayed depend on the overlap value defined in the office code configuration
Private Extension	yes	digits displayed depend on the overlap value defined in the office code configuration
BC Federation	no	
Comm. System	no	column appears only when <i>All comm.</i> Systems are in display
Unique	no	Unique numbers are the ones that belong to non VNR OpenScape 4000 switches
ONS	no	yes or no
Virtual Node ID	no	Virtual Node IDs are applicable only to VNR OpenScape 4000 switches

- 4) Click on the subscriber you wish to edit.
- 5) Change the resource settings.

NOTICE:

Only the **Address Translation Context** attribute can be modified for the Voice Subscriber of a communication system in the CMP. All other fields are *read only*.

- 6) Click on **Save** to copy the entries to the system's database.

6.6.7 How to Display Media Server Office Codes

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a Media Server can only be added or deleted in the CMP they can't be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Office Codes**.

A list of all Office Codes appears in the work area.

- 3) Following attributes of the Office Code are displayed in the workspace.

Attribute	Sorting available
Office Code / Node Access Code	yes
Type	yes
Overlap	no

- 4) Click on the **Office Code** you wish to display.
- 5) The **Private Office Code** or **Public Office Code** info page pops up.
All fields are read-only.
- 6) Click on the **Close** button to close the page.

6.6.8 How to Display Media Server Office Codes

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a Media Server can only be added or deleted in the CMP they can't be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree click, click on **Devices > Media server > Office Codes**.

A list of all Office Codes appears in the work area.

- 3) Following attributes of the Office Code are displayed in the workspace.

Attribute	Sorting available
Office Code / Node Access Code	yes
Type	yes
Overlap	no

- 4) Click on the **Office Code** you wish to display.
- 5) The **Private Office Code** or **Public Office Code** info page pops up.
All fields are read-only.
- 6) Click on the **Close** button to close the page.

6.6.9 How to Add Media Server Office Code

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a Media Server can only be added or deleted in the CMP they can't be modified.

- You have already an established CSTA connection.
- You have to set a Default Address Translation Context in.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Office Codes**.

A list of all Office Codes appears in the work area.

- 3) Click on the **Add** button.

Following fields must be filled in:

L2 code - L1 code - L0 Code for a **Private** Office Code

and respectively

Country code – Area code – Local Office Code for a **Public** Office Code

An office code may contain a so-called **overlap**. This overlap specifies if and to what extent the office code and the associated extensions overlap.

Example: A fully qualified phone number be 492404902100. The office code is 492404902 and the extension 2100. In this example, one digit of

the extension and office code overlap – namely digit 2 . The **overlap** in this example is thus 1.

- 4) Click on **Save** to copy the entries to the system's database.

6.6.10 How to Delete Media Server Office Codes

All office codes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Office Codes of a Media Server can only be added or deleted in the CMP they can't be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Office Codes**.

A list of all Office Codes appears in the work area.
- 3) Click the check box of the Office Code you wish to Delete.
- 4) Click on **Delete** to remove the office code from the system's database.

6.6.11 How to Add Media Server Prefixes

All prefixes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Prefixes of a Media Server can only be added or deleted in the CMP, they can't be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Prefixes**.

A list of all Prefixes appears in the work area.

3) Click on the **Add** button.

The dialog with the prefix settings opens and depending on the Prefix Type (Private or Public) following attributes can be filled in:

Type Private	Type Public
L2 Prefix	International Prefix
L2 Network Access Code	International Network Access Code (mandatory)
L1 Prefix	National Prefix
L1 Network Access Code	National Network Access Code
L0 Prefix	Subscriber Prefix
L0 Network Access Code (mandatory)	Subscriber Network Access Code

NOTICE:

L0 Network Access Code is a mandatory field for a Private Media Server Prefix and International Network Access Code is a mandatory field for a Public Media Server Prefix.

4) Click on **Save** copy the entries to the system's database.

6.6.12 How to Display Media Server Prefixes

All prefixes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Prefixes of a Media Server can only be added or deleted in the CMP, they can't be modified.

Step by Step

1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.

2) In the navigation tree click, click on **Devices > Media server > Prefixes**.

A list of all Prefixes configured in the selected communication system appears in the work area.

3) Following attributes of the Prefixes are displayed in the workspace depending on the Prefix Type (Private or Public)

Prefix Id	Prefix Id
Type Private	Type Public

L2 Prefix	International Prefix
L2 Network Access Code	International Network Access Code
L1 Prefix	National Prefix
L1 Network Access Code	National Network Access Code
L0 Prefix	Subscriber Prefix
L0 Network Access Code	Subscriber Network Access Code

6.6.13 How to Delete Media Server Prefixes

All prefixes of a Communication System are synchronized in to the CMP database.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

NOTICE: Prefixes of a Media Server can only be added or deleted in the CMP, they can't be modified.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Prefixes**.
A list of all Prefixes configured in the selected communication system appears in the work area.
- 3) Click the check box of the Prefix you wish to delete.
- 4) Click on **Delete** to remove the Prefix from the system's database.

6.6.14 How to Display Media Server Conference Devices

All Conference Devices of the selected domain can be administered in CMP.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree click, click on **Devices > Media server > Conference Devices**.

The list of all Conference Devices within the selected domain are displayed in the workspace with the following attributes:

Normalized Number	sorting possible
Public Extension	sorting possible
Private Extension	sorting possible
Media Servers	sorting possible

- 3) If you wish to display a Conference Device or a list of Conference Devices, specify in the display filter a search criterion that the desired resource matches and click on Go or select the Conference Devices you wish to display and click on **Show selected items**.

6.6.15 How to Add Media Server Conference Device

All Conference Devices of the selected domain can be administered in CMP.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.
- Media Server Office Codes and Prefixes must be configured

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Conference Devices**.

The list of all Conference Devices within the selected domain are displayed in the workspace with the following attributes:

Normalized Number	sorting possible
Public Extension	sorting possible
Private Extension	sorting possible
Media Servers	sorting possible

- 3) Click on the **Add** button and the dialog with the prefix settings opens and following attributes can be filled in:
 - a) Tick the **offboard** box to select the Media Server.
 - b) Choose from the pull down menu the **Media Server Type**.
 - c) For a Public Number fill in the following fields: **Office Code, Prefix, Extension**.
 - d) For a Private Number fill in the following fields: **Office Code , Prefix , PN Extension**.
- 4) Click on **OK** to copy the entries to the system's database.

6.6.16 How to Delete Media Server Conference Device

All Conference Devices of the selected domain can be administered in CMP.

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Devices > Media server > Conference Devices**.
- 3) Select the Conference Devices you wish to delete and click on the **Delete** button.

The Conference Devices are removed from the conference device list

6.7 Address Translation Context Overview

All Services including UC Services need to ensure that any external address data is normalized before it is passed through the system to other services. The boundary are the services which get information from clients.

In UC we need the ability to translate in specific translation contexts and have references to one or more address translation contexts.

Address Translation Context can be assigned to:

- A Voice Portal Number
- A Media Server endpoint
- A Voice Subscriber
- A range of OpenScape 4000 station extensions

In case multiple Office Codes have been configured on the same OpenScape 4000 the extension ranges must be mapped to address Translation Contexts containing the Office Codes of these extensions.

This mapping is done in the **Address Translation Station Routing** page.

Repetition of extension is not allowed so each extension appears only once and is mapped to a unique Office Code.

Media Server Office Codes can only be configured if a default Address Translation Context is defined.

NOTICE: The Address Translation Context has a flag to identify the default context.

6.7.1 How to Add Address Translation Context

How to add an Address Translation Context:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Address Translation Context**.

A list of all **Address Translation Contexts** appears in the work area with the following info:

Name	Context Name
Description	Context Description
Switch	The switch for which the Context is configured
Default	Indication if the context is configured as the default Context. Only one of the Contexts can be set as default.

- 3) Click on the **Add** button.
The dialog with the Context settings opens.
- 4) Click on the **Context** tab to configure the Context and Test the Translation.
 - a) Tick the **default context** box if you want to configure the Translator Context as default.
 - b) Enter the Context **Name**.
 - c) Choose the **Switch** for which the Context will be configured.
 - d) Enter a Context **Description**.
 - e) Choose at least one office code for the translation context from the Public, Private and Unknown office code pull down menus.
 - f) Choose the Translation type.
 - g) Enter the number format you will translate.

- 5) Choose the **Translator type** with the chosen configured groovy script you want to test.

- 6) Enter the **Number** you want to test.

- 7) Click on the **Test Translation** button.

The test result appears in the **Result** field.

- 8) Click on the **UI & IT Norm.** tab to see the list of Translation Types and choose the appropriate groovy script.

- The available Translation Types are the following:

Conversion Type	Name	Description
CS Localization	SERVICE_ID	Produce a CSTA Service ID for invoking requests

CS Normalization	TARGET	Produce a dialable string
CS Normalization	DEVICE	Standard normalization of a device provided in a CSTA event
CS Normalization	TRUNK	Normalization for Media Server purposes
UI Localization	GUI_PRESENTATION	Separate Numbering Plan components with brackets/ parentheses for display
UI Localization	SHORTEST_DIALABLE	Produce a dialable string
UI Normalization	FAIL_ON_ERROR	Exception when the system is unable to produce a result
UI Normalization	PASS_THROUGH_ON_ERROR	ERROR will be sent as is when unable to produce result
UI Normalization	EXTENDED	When unable to translate consult OSV via SOAP interface or look up the imported routing table of the OpenScape 4000
UI Normalization	DIRECTORY	Normalization of numbers coming from a directory.

- The conversion type used for the Context Translation have the following values:

CS Localization: Conversion of a dialable number coming from a Communication System to the Normalized format

CS Normalization: Conversion of a Normalized number coming from a Communication System to a dialable format

UI Localization: Conversion of a dialable number coming from clients to the Normalized format

UI Normalization: Conversion of a Normalized number coming from a Communication System to a dialable format

NOTICE: Dialable number is a number that can be dialed from a device in order to reach a destination.

NOTICE: A Fully Qualified Number (FQN) or a Normalized number is a number that cannot be confused with another.

NOTICE: An Address Translator Context is not required to have a groovy script if not necessary.

- 9) Choose the groovy script you want to map to the relative Translation type. You may want to test the groovy script in the Test Translation area before saving the settings.
- 10) Click on **Save** to copy the entries to the system's database.

6.7.2 How to Display Address Translation Contexts

How to display the Address Translation Context list:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Address Translation Context**.

A list of all **Address Translation Contexts** appears in the work area with the following info:

Name	Context Name
Description	Context Description
Switch	The switch for which the Context is configured

Default	Indication if the context is configured as the default Context. Only one of the Contexts can be set as default.

6.7.3 How to Edit Address Translation Context

How to add an Address Translation Context:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Address Translation Context**.

A list of all **Address Translation Contexts** appears in the work area with the following info:

Name	Context Name
Description	Context Description
Switch	The switch for which the Context is configured
Default	Indication if the context is configured as the default Context. Only one of the Contexts can be set as default.

- 3) Click on the **Edit** button.
The dialog with the Context settings opens.
- 4) Click on the **Context** tab to configure the Context and Test the Translation.
 - a) Tick the **default context** box if you want to configure the Translator Context as default.
 - b) Enter the Context **Name**.
 - c) Choose the **Switch** for which the Context will be configured.
 - d) Enter a Context **Description**.
 - e) Choose at least one office code for the translation context from the Public, Private and Unknown office code pull down menus.
 - f) Choose the Translation type.
 - g) Enter the number format you will translate.
- 5) Choose the **Translator type** with the chosen configured groovy script you want to test.
- 6) Enter the **Number** you want to test.
- 7) Click on the **Test Translation** button.
The test result appears in the **Result** field.

- 8) Click on the **UI & IT Norm.** tab to see the list of Translation Types and choose the appropriate groovy script.

- The available Translation Types are the following:

Conversion Type	Name	Description
CS Localization	SERVICE_ID	Produce a CSTA Service ID for invoking requests
CS Localization	TARGET	Produce a dialable string
CS Normalization	DEVICE	Standard normalization of a device provided in a CSTA event
CS Normalization	TRUNK	Normalization for Media Server purposes
UI Localization	GUI_PRESENTATION	Separate Numbering Plan components with brackets/ parentheses for display
UI Localization	SHORTEST_DIALABLE	Produce a dialable string
UI Normalization	FAIL_ON_ERROR	Exception when the system is unable to produce a result
UI Normalization	PASS_THROUGH_ON_ERROR	ERROR will be sent as is when unable to produce result
UI Normalization	EXTENDED	When unable to translate consult OSV via SOAP interface or look up the imported routing table of the OpenScape 4000
UI Normalization	DIRECTORY	Normalization of numbers coming from a directory.

- The conversion type used for the Context Translation have the following values:

CS Localization: Conversion of a dialable number coming from a Communication System to the Normalized format.

CS Normalization: Conversion of a Normalized number coming from a Communication System to a dialable format.

UI Localization: Conversion of a dialable number coming from clients to the Normalized format.

UI Normalization: Conversion of a Normalized number coming from a Communication System to a dialable format.

NOTICE: Dialable number is a number that can be dialed from a device in order to reach a destination.

NOTICE: A Fully Qualified Number (FQN) or a Normalized number is a number that cannot be confused with another.

NOTICE: An Address Translator Context is not required to have a groovy script if not necessary.

- 9) Choose the groovy script you want to map to the relative Translation type. You may want to test the groovy script in the Test Translation area before saving the settings.
- 10) Click on **Save** to copy the entries to the system's database.

6.7.4 How to Add an Address Translation Station Routing

How to add an Address Translation Station Routing:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Address Translation Station Routing**.

A list of all **conversions** appears in the work area with the following info:

Context	Address Translation Context
Communication System	Communication System
Range	The extension range that is mapped to the Address Translation Contexts.
Type	Extension Type

- 3) Click on the **Add** button.
The dialog with the Station Routing settings opens.
- 4) Choose the **Communication System** in which you will configure the Station Routing.
- 5) Choose the **Extension type**.
- 6) Choose the **Context** you will use for mapping the extension range below
- 7) Enter the **Range Start** and **Range Stop** for defining the extensions you will map to this Context.
- 8) Click on **Save** to copy the entries to the system's database

6.7.5 How to Display Address Translation Station Routing

How to display Address Translation Station Routing conversions:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Address Translation Station Routing**.

A list of all **conversions** appears in the work area with the following info:

Context	Address Translation Context
Communication System	Communication System
Range	The extension range that is mapped to the Address Translation Contexts.
Type	Extension Type

6.8 HiPath OpenScape Configuration

If you use OpenScape UC Application, CSTA connections must be configured and administered between OpenScape UC Application and the communications systems used.

NOTICE: The HiPath OpenScape configuration is only used when you deploy OpenScape UC Application.

Via these connections the following features are enabled.

- Monitoring the status of terminal devices
- Monitoring and controlling connections in the relevant communications system

Configuring a CSTA connection also activates a function that copies the subscriber information of the communications system as resources to OpenScape UC Application.

As soon as such a resource is assigned to a UC Application user, OpenScape UC Application sets a CTI monitor point in the relevant communications system for the relevant subscriber and starts CTI monitoring for him/her.

6.8.1 How to Display OpenScape Voice switch Connections

How to display OSV switch connections:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > OS Voice**.

A dialog that displays all configured OpenScape Voice connections opens.

6.8.2 How to Add an OpenScape Voice Connection

How to Add an OSV switch connection:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > OS Voice**.

In case there is a need for Video Call via webClient, the administrator should select OpenScape Voice Vx Video. (e.g. OpenScape Voice V9.0 Video).

When OpenScape Voice Connection is configured without Video, the makeCall requests are initiated without requesting video. Note that OSV handles these CTI call as audio call, as the default value, if mediaCallCharacteristics is not included.

NOTICE: Select the correct OpenScape Version.

A dialog that displays all configured OpenScape Voice connections opens.

- 3) Click on **Add**.

The dialog with the link settings opens.

- 4) Select under **Switch** the OpenScape Voice system to which OpenScape UC Application is to be connected.
- 5) Select under **Version** the version of the OpenScape Voice system to be connected to the OpenScape UC Application.
- 6) Enter the IP address for the CSTA interface provided by OpenScape Voice in the **CSTA access configuration** area under **IP/Hostname**.
- 7) Specify the port number for the CSTA communication in the **CSTA access configuration** area under **Port**. This is port number 1040 by default.
- 8) If you want to use an alternative CSTA interface in the selected OpenScape Voice system, specify the IP address of the alternative CSTA interface in the **CSTA access configuration** area under **IP/Hostname (alternative)**.
- 9) If you use an alternative CSTA interface, specify the port number for the CSTA communication in the **CSTA access configuration** area under **Port (alternative)**. This is port number 1040 by default.
- 10) If you use OpenScape UC Application with several nodes, select the OpenScape computer system to be connected with OpenScape Voice in the **BCom configuration** area under **Node**.
- 11) Enter the IP address for the SOAP communication in the **SOAP access configuration** area under **IP/Hostname**.
- 12) Specify the port number used by OpenScape UC Application for translating phone numbers in the **SOAP access configuration** area under **Port**. The recommended SOAP port is 8768.

NOTICE:

Secure port numbers, such as 8757 and 8758 are not allowed.

- 13) If you want to use an alternative SOAP interface in the selected OpenScape Voice system, specify the IP address of the alternative SOAP interface in the **SOAP Access Configuration** area under **IP/Hostname (alternative)**.
- 14) If you use an alternative SOAP interface, specify the port number for the SOAP communication in the **SOAP access configuration** area, under **Port (alternative)**. This is insecure port number 8767 by default.

NOTICE: Secure port numbers, such as 8757 and 8758 are not allowed.

- 15) Specify a **Listening IP for UDP, TCP and TLS** in the **Signaling Protocol** area.
- 16) Specify an alternative IP under **Listening IP (alternative) for UDP, TCP and TLS**.
- 17) Enter your port in **Node TCP/UDP Port** field and a **TLS port** in the **TLS Port** field.
- 18) Enter your protocol version number in **Protocol Version**.
- 19) Click on **Save** to copy the entries to the system's database.

The new connection is saved and displayed in the connection list.

6.8.3 How to Display Media Server Connections

How to Display Media Server Connections:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > Media Server**.

A dialog that displays all configured Media Server connections opens.

6.8.4 How to Add a Media Server Connection

How to add a Media Server Connection:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > Media Server**.

A dialog that displays all configured Media Server connections opens.

- 3) Click on **Add**.

The dialog with the connection cluster settings opens.

- 4) Select under **Media-Server** the media server you want to connect with OpenScape UC Application.
- 5) Select under Version the entry **Global Number Format (GNF)**.
- 6) Click on **Add**.

The dialog with the link settings opens.

- 7) Enter the name for the new connection under **Connection Name**.

Under this name the connection is later on administered in the Common Management Platform.

- 8) Under BCom Provider select the entry MSProv1.
- 9) Select **Save**.

The new Media Server connection is now displayed in the window of the Media Server connection cluster.

- 10) Click on **Save** to copy the entries to the system's database.

The new connection is saved and displayed in the connection list.

6.9 LDAP Connection

Via the LDAP connection you connect OpenScape UC Application external LDAP directories. In this way you can provide an LDAP-based global contact list to OpenScape users.

NOTICE: You can only deploy an LDAP connection when you use OpenScape UC Application.

The LDAP connection is based on the OpenScape UC Application directory service, which supports a general LDAP-based search feature. But entries of a connected directory can neither be created nor modified or deleted from within the OpenScape system.

Field assignments (mapping) of the LDAP connection

The information of a connected LDAP directory can be assigned to the single elements of the OpenScape UC Application data structure.

NOTICE: The clients of OpenScape UC Application do not display all of the database fields that are available and mapped in the LDAP connector.

The following table shows an example assignment for the LDAP connection of an Active Directory. The following properties apply for the system environment:

IP address of the AD server:	139.21.211.216
Port used:	389
User name for the directory access:	adtester
User domain:	adtest
Password for the directory access: ¹⁷	NFNpZW1lbnMh
Search base:	OU=Testuser,DC=adtest,DC=local

NOTICE: In a Window 2003 Active Directory domain with more than one domain controller you have to configure the LDAP connector to communicate with the global catalog server. Doing so, you have to configure port 3268 for non-encrypted communication or port 3269 for communication using SSL.

Property name	Active Directory assignment	Property description
AttrMap.Alias		Alternative contact name
AttrMap.BuildingNumber	building	Building number
AttrMap.Business	telephoneNumber	Phone number (business) of the contact

¹⁷ The password is base64-coded and must be entered in coded format. The base64 coding can be performed on the following website: http://www.php-einfach.de/base64_generator.php

System management for the components of OpenScape UC Application

AttrMap.Business2	alternatePhone	Alternative phone number (business) of the contact
AttrMap.Business2Normalized		Alternative phone number (business) of the contact in a normalized format
AttrMap.BusinessFax	faxNumber	Fax number (business) of the contact
AttrMap.BusinessFaxNormalized		Fax number (business) of the contact in a normalized format
AttrMap.BusinessNormalized		Phone number (business) of the contact in a normalized format
AttrMap.City	localityInternational	City where the company is located
AttrMap.CompanyName	company	Company name
AttrMap.CountryCode	c	Country where the company is located
AttrMap.Department	department	Company department
AttrMap.Description		Short description
AttrMap.DisplayName	displayName	Display name of the contact
AttrMap.Email	mail	E-mail address of the contact
AttrMap.Email2		Alternative e-mail address of the contact
AttrMap.Gender	gender	Gender of the contact
AttrMap.GivenName	givenName	First name of the contact
AttrMap.Home		Private phone number of the contact
AttrMap.HomeNormalized		Private phone number of the contact in normalized format
AttrMap.HomeUrl	labeledURI	Home page address of the company
AttrMap.ImAddress		Instant-Messaging address of the contact
AttrMap.LastName (mandatory if you are going to add this LDAP contact to you private contact)	sn	Last name of the contact
AttrMap.LinkToSymMetaDirectory		

AttrMap.MiddleName		Middle name of the contact
AttrMap.Mobile	mobile	Mobile phone number of the contact
AttrMap.MobileNormalized		Mobile phone number of the contact in normalized format
AttrMap.Notice		Notice
AttrMap.Phone (mandatory if you want to lookup contacts by their phone numbers)	telephoneNumber,alternateTelephone	Database fields that may contain phone numbers
AttrMap.Picture		Image information of the contact NOTE: Max. size for image file: 15KB
AttrMap.PostalCode		Zip code of the place where the company is located
AttrMap.RoomNumber	roomNumber	Room number in the company building
AttrMap.Salutation	personalTitle	Personal salutation of the contact
AttrMap.StateOrProvince		State /province in which the company is located
AttrMap.Street		Street in which the company is located
AttrMap.Title	graduateTitle	Title of the contact
AttrMap.VanityCode		Vanity code of the contact
AttrMap.VdsId (mandatory or not used)	scdId	Field of the LDAP directory that contains a unique data-ID. If the LDAP directory does not include such a field, set the useDNasID property to true.
Connection Properties		
connection.displayName	Company directory	Display name of the directory in the client
connection.followReferrals (mandatory)	false	Defines whether references of the LDAP directory are gone into.
connection.password	NFNpZW1lbnMh	Password for the directory access

searchBase (mandatory)	OU=Testuser,DC=adtest,DC=adtest	Search base for the LDAP directory accessFor newer versions of LDAP connector this field can be empty
connection.serverURL (mandatory)	139.21.211.216:389	<IP address>:<port> or <host name>:<port> of the LDAP server
connection.username	adtest\adtester	User name for the directory access
connection.useSSL (mandatory)	false	Defines whether SSL is used for the communication.
ldapVersion (if this property is not set then the provider first attempts to bind using version 3 and if a protocol error is received from the server it uses version 2)	3	Version of the LDAP directoryIMPORTANT: This value must not be changed.
maxRecords (must be >0)	600	Maximum number of data records that the LDAP directory delivers upon a search requestThe maximum number of records returned may also be limited on the LDAP server
searchMask		Search mask for the LDAP directory access
useDNasID (mandatory)	false	Defines whether the distinguished name of an LDAP entry is used as unique ID in case of a directory search. This property must be set to true if the connected LDAP directory does not have a field with unique data ID.
concurrentRequestLimit	10	IMPORTANT: This value must not be changed.
poolDebugLevel		which LDAP connection information shall be loggedIMPORTANT: This value is only for internal use.

6.9.1 How to Display Settings for LDAP Connection

How to display LDAP connection settings:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > LDAP**.

A dialog that displays all configured LDAP connections opens.

6.9.2 How to Add an LDAP Directory Connection

How to Add an LDAP directory Connection:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > LDAP**.

A dialog that displays all configured LDAP connections opens.

- 3) Click on **Add**.

A window opens that displays the settings of the LDAP connection.

- 4) Navigate to Connection Properties area and fill in the fields.
- 5) Specify under the **connection.displayName** connection property the name under which the LDAP directory is to be displayed in the OpenScape clients.
- 6) Specify under the **connection.serverURL** connection property the following data and, in doing so, separate them with a colon:
 - a) IP address under which the LDAP directory server can be reached.

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.
 - b) Port via which the LDAP connector is to exchange data with the LDAP directory server.

NOTICE:

In a Windows 2003 Active Directory domain with more than one domain controller you have to configure the LDAP connector to communicate with the global

catalog server. Doing so, you have to configure port 3268 for non-encrypted communication or port 3269 for communication using SSL.

- 7) If the LDAP connector of OpenScape UC Application is not to anonymously access the LDAP directory, proceed as follows:
 - a) Specify under the **connection.username** connection property the user account that is to be used instead.
 - b) Specify under the **connection.password** connection property the password for the user account used.

NOTICE: In case of a connected Active Directory for Windows 2003 Server, deploying a default domain user is sufficient. The user need not have administrative privileges.

- 8) Specify under the **connection.useSSL** connection property whether communication between LDAP connector and LDAP directory is to be encrypted via SSL.
 - If the communication is to be encrypted via SSL, enter `true` in the field of this property.

NOTICE: If you want to use SSL, you need to specify the port for SSL under the **connection.serverURL** property.

- If the communication is not to be encrypted via SSL, enter `false` in the field of this property.
- 9) Specify the search base with which the LDAP connector is to access the LDAP directory under the **searchBase** connection property.

NOTICE: A search base must always be a subdirectory.

- 10) Specify under the **searchMask** connection property the search mask the LDAP connector is to use for each search request.

The search mask must contain the `#s` expression at least once. The LDAP connector replaces this expression with the search filter when a search request is placed.
- 11) Under the **maxRecords** connection property, specify the maximum number of data records the LDAP directory is to deliver upon a search request.

If an appropriate limit has already been configured in the LDAP directory, the **maxRecords** setting is noneffective.
- 12) Specify under the **useDNasID** connection property whether the distinguished name of an LDAP entry is to be used as unique ID in case of a directory search.

NOTICE: This connection property must be set to true if the connected LDAP directory does not have a field with unique data ID.

- 13) Specify under the **connection.followReferrals** connection property whether references to the LDAP directory are to be pursued.
- If references to the LDAP directory are to be pursued, enter `true` in the field of this property.
 - If references to the LDAP directory are not to be pursued, enter `false` in the field of this property.

- 14) Specify under the **AttrMap.Phone** mapping property which LDAP directory database fields may contain phone numbers. If you want to specify several database fields, separate them by comma.

telephoneNumber,alternatePhone,mobile

If OpenScape UC Application searches the LDAP directory based on a phone number, only the database fields of the LDAP directory containing this phone number are considered for the search.

- 15) Specify under the **poolDebugLevel** mapping property, which LDAP connection information shall be logged.
- If no LDAP connection information shall be logged, leave the field of this property empty.
 - If information about setting up and closing LDAP connections shall be logged, enter `fine` in the field of this property.
 - If all information about LDAP connections shall be logged, enter `all` in the field of this property.

The logged data is stored in the following file: `/var/siemens/common/log/osgi.err`

- 16) From the Connection Properties area the following fields are mandatory:

Property Name	Active Directory assignment	Property Description
connection.followReferrals (mandatory)	<code>false</code>	Defines whether references of the LDAP directory are gone into.
searchBase (mandatory)	OU=Testuser, DC=adtest, DC=local	Search base for the LDAP directory access For newer versions of LDAP connector this field can be empty
connection.serverURL (mandatory)	139.21.211.216:389	<IP address>:<port> or <host name>:<port> of the LDAP server
connection.useSSL (mandatory)	<code>false</code>	Defines whether SSL is used for the communication.

Property Name	Active Directory assignment	Property Description
maxRecords (must be >0)	600	Maximum number of data records that the LDAP directory delivers upon a search request The maximum number of records returned may also be limited on the LDAP server
useDNasID (mandatory)	false	Defines whether the distinguished name of an LDAP entry is used as unique ID in case of a directory search. This property must be set to true if the connected LDAP directory does not have a field with unique data ID.

- 17) Navigate to the Mapping Property area and enter the required fields according to the following table:

Property Name	Active Directory assignment	Property Description
AttrMap.Alias		Alternative contact name
AttrMap.BuildingNumber	building	Building number
AttrMap.Business	telephoneNumber	Phone number (business) of the contact
AttrMap.Business2	alternatePhone	Alternative phone number (business) of the contact
AttrMap.Business2Normalized		Alternative phone number (business) of the contact in a normalized format
AttrMap.BusinessFax	faxNumber	Fax number (business) of the contact
AttrMap.BusinessFaxNormalized		Fax number (business) of the contact in a normalized format
AttrMap.BusinessNormalized		Phone number (business) of the contact in a normalized format

AttrMap.City	localityInternational	City where the company is located
AttrMap.CompanyName	company	Company name
AttrMap.CountryCode	c	Country where the company is located
AttrMap.Department	department	Company department
AttrMap.Description		Short description
AttrMap.DisplayName	displayName	Display name of the contact
AttrMap.Email	mail	E-mail address of the contact
AttrMap.Email2		Alternative e-mail address of the contact
AttrMap.Gender	gender	Gender of the contact
AttrMap.GivenName	givenName	First name of the contact
AttrMap.Home		Private phone number of the contact
AttrMap.HomeNormalized		Private phone number of the contact in normalized format
AttrMap.HomeUrl	labeledURI	Home page address of the company
AttrMap.ImAddress		Instant-Messaging address of the contact
AttrMap.LastName (mandatory if you are going to add this LDAP contact to you private contact)	sn	Last name of the contact
AttrMap.LinkToSymMetaDirectory		
AttrMap.MiddleName		Middle name of the contact
AttrMap.Mobile	mobile	Mobile phone number of the contact
AttrMap.MobileNormalized		Mobile phone number of the contact in normalized format
AttrMap.Notice		Notice
AttrMap.Phone (mandatory if you want to lookup contacts by their phone numbers)	telephoneNumber,alternativeTelephone	Telephone numbers fields that may contain phone numbers

AttrMap.Picture		Image information of the contact NOTE: Max. size for image file: 15KB
AttrMap.PostalCode		Zip code of the place where the company is located
AttrMap.RoomNumber	roomNumber	Room number in the company building
AttrMap.Salutation	personalTitle	Personal salutation of the contact
AttrMap.StateOrProvince		State /province in which the company is located
AttrMap.Street		Street in which the company is located
AttrMap.Title	graduateTitle	Title of the contact
AttrMap.VanityCode		Vanity code of the contact
AttrMap.VdsId (mandatory or not used)	scdId	Field of the LDAP directory that contains a unique data-ID. If the LDAP directory does not include such a field, set the useDNasID property to true.
Connection Properties		
connection.displayName	Company directory	Display name of the directory in the client
connection.followReferrals (mandatory)	false	Defines whether references of the LDAP directory are gone into.
connection.password	NFNpZW1lbnMh	Password for the directory access
searchBase (mandatory)	OU=Testuser,DC=adtest,DC=de	Search base for the LDAP directory access For newer versions of LDAP connector this field can be empty
connection.serverURL (mandatory)	139.21.211.216:389	<IP address>:<port> or <host name>:<port> of the LDAP server
connection.username	adtest\adtester	User name for the directory access
connection.useSSL (mandatory)	false	Defines whether SSL is used for the communication.

ldapVersion (if this property is not set then the provider first attempts to bind using version 3 and if a protocol error is received from the server it uses version 2)	3	Version of the LDAP directory IMPORTANT: This value must not be changed.
maxRecords (must be >0)	600	Maximum number of data records that the LDAP directory delivers upon a search request The maximum number of records returned may also be limited on the LDAP server
searchMask		Search mask for the LDAP directory access
useDNasID (mandatory)	false	Defines whether the distinguished name of an LDAP entry is used as unique ID in case of a directory search. This property must be set to true if the connected LDAP directory does not have a field with unique data ID.
concurrentRequestLimit	10	IMPORTANT: This value must not be changed.
poolDebugLevel		which LDAP connection information shall be logged IMPORTANT: This value is only for internal use.

connection.defaultConnectTimeout		These properties specify the default connect and read timeout (resp.) for the protocol handler used by java.net.URLConnection.defaultConnectTimeout specifies the timeout (in milliseconds) to establish the connection to the host. For example for http connections it is the timeout when establishing the connection to the http server. For ftp connection it is the timeout when establishing the connection to ftp servers.	
connection.defaultReadTimeout		defaultReadTimeout specifies the timeout (in milliseconds) when reading from input stream when a connection is established to a resource. See also https://docs.oracle.com/javase/7/docs/technotes/guides/net/properties.html .	
connection.defaultSearchTimeLimit		default time limit for a search, translates internally to LdapConstants.PROPERTY_CONNECTION_TIMEOUT	
connectionTimeout		The com.sun.jndi.ldap.connect.timeout environment property is used to specify a timeout period for establishment of the LDAP connection. This property affects the TCP timeout when opening a connection to an LDAP server.	

readTimeout		When an LDAP request is made by a client to a server and the server does not respond for some reason, the client waits forever for the server to respond until the TCP timeouts. On the client-side what the user experiences is essentially a process hang. In order to control the LDAP request in a timely manner, a read timeout can be configured or the Sun JNDI/LDAP Service Provider since Java SE 6. The environment property: <code>com.sun.jndi.ldap.read.timeout</code> can be used to specify the read timeout for an LDAP operation.
searchTimelimit		A time limit on a search places an upper bound on the amount of time that the search operation will block waiting for the answers. This is useful when you don't want to wait too long for an answer.
httpProxyDomain		defines the Proxy Domain
httpProxyHost		defines the Proxy host
httpProxyPassword		defines the Proxy password, Base 64 decoded
httpProxyPort		defines the Proxy Port
httpProxyUser		defines the Proxy user
httpSecurityProtocol		defines the protocol used for security (SSL, TLS version)

18) Click on **Save** to copy the entries to the system's database.

19) Restart the **LDAP Connector Service** for the modifications to take effect.

The new LDAP connection is added in the Global List ¹⁸.

¹⁸ Navigate to Configuration > Unified Communication > Accounts > Contact Settings > Global List

6.9.3 How to Edit an LDAP Directory Connection

How to Configure the Connection to the LDAP directory:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > LDAP**.

A dialog that displays all configured LDAP connections opens.

- 3) Select the check box of the LDAP connection the settings of which you want and click on **Edit**.

A window opens that displays the settings of the LDAP connection.

- 4) Specify under the **connection.displayName** connection property the name under which the LDAP directory is to be displayed in the OpenScape clients.
- 5) Specify under the **connection.serverURL** connection property the following data and, in doing so, separate them with a colon:
 - a) IP address under which the LDAP directory server can be reached.

If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.
 - b) Port via which the LDAP connector is to exchange data with the LDAP directory server.

NOTICE: In a Windows 2003 Active Directory domain with more than one domain controller you have to configure the LDAP connector to communicate with the global catalog server. Doing so, you have to configure port 3268 for unencrypted communication or port 3269 for communication using SSL.

- 6) If the LDAP connector of OpenScape UC Application is not to anonymously access the LDAP directory, proceed as follows:
 - a) Specify under the **connection.username** connection property the user account that is to be used instead.
 - b) Specify under the **connection.password** connection property the password for the user account used.

In case of a connected Active Directory for Windows 2003 Server, deploying a default domain user is sufficient. The user need not have administrative privileges.

- 7) Specify under the **connection.useSSL** connection property whether communication between LDAP connector and LDAP directory is to be encrypted via SSL.
- If the communication is to be encrypted via SSL, enter `true` in the field of this property.

NOTICE: If you want to use SSL, you need to specify the port for SSL under the **connection.serverURL** property.

- If the communication is not to be encrypted via SSL, enter `false` in the field of this property.
- 8) Specify the search base with which the LDAP connector is to access the LDAP directory under the **searchBase** connection property.
- If you want to specify several search bases, separate them by comma.

NOTICE: A search base must always be a subdirectory.

- 9) Specify under the **searchMask** connection property the search mask the LDAP connector is to use for each search request.
- The search mask must contain the `#s` expression at least once. The LDAP connector replaces this expression with the search filter when a search request is placed.
- 10) Under the **maxRecords** connection property, specify the maximum number of data records the LDAP directory is to deliver upon a search request.
- If an appropriate limit has already been configured in the LDAP directory, the `maxRecords` setting is noneffective.
- 11) Specify under the **useDNasID** connection property whether the distinguished name of an LDAP entry is to be used as unique ID in case of a directory search.

NOTICE: This connection property must be set to `true` if the connected LDAP directory does not have a field with unique data ID.

- 12) Specify under the **connection.followReferrals** connection property whether references to the LDAP directory are to be pursued.
- If references to the LDAP directory are to be pursued, enter `true` in the field of this property.
 - If references to the LDAP directory are not to be pursued, enter `false` in the field of this property.
- 13) Specify under the **AttrMap.Phone** mapping property which LDAP directory database fields may contain phone numbers. If you want to specify several database fields, separate them by comma.

telephoneNumber,alternatePhone,mobile

If OpenScape UC Application searches the LDAP directory based on a phone number, only the database fields of the LDAP directory containing this phone number are considered for the search.

- 14) Specify under the **poolDebugLevel** mapping property, which LDAP connection information shall be logged.
 - If no LDAP connection information shall be logged, leave the field of this property empty.
 - If information about setting up and closing LDAP connections shall be logged, enter `fine` in the field of this property.
 - If all information about LDAP connections shall be logged, enter `all` in the field of this property.

The logged data is stored in the following sequence: `/var/siemens/common/log/osgi.err`

- 15) Click on **Save** to copy the entries to the system's database.
- 16) Restart the **LDAP Connector Service** for the modifications to take effect.

6.9.4 How to Clone an LDAP Directory Connection

How to Configure the Connection to the LDAP directory:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > LDAP**.

A dialog that displays all configured LDAP connections opens.
- 3) Select the LDAP connection that you want to clone and click on the action menu.

A list of all available actions is displayed.
- 4) Click on **Clone**.

A window opens that displays the settings of the LDAP connection.
- 5) Make all the changes you want as if creating a new LDAP connection and click on **Save**.

NOTICE: The default name assigned to the cloned LDAP connection in the field **connection.displayName** is *CopyOf name of initial LDAP connection*.

6.9.5 How to Delete an LDAP Directory Connection

How to Delete an LDAP directory Connection:

Prerequisites

- You use OpenScape UC Application in your OpenScape system.
- Adequate administrative permissions.

Step by Step

- 1) On the **Configuration** navigate tab click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree click, click on **Configuration > Connections > LDAP**.
A dialog that displays all configured LDAP connections opens.
- 3) Select the check box of the LDAP connection you want to remove and click on **Delete**.

You are prompted to confirm the deletion of the connection.

NOTICE:

The system requirement is that we have at least one LDAP connection. Therefore if you attempt to delete the only LDAP connection that appears in the LDAP Connection list, an error message appears and deletion is not allowed.

6.9.6 Using avatar pictures in a UC system on a LDAP Directory Connection

User avatar pictures coming from an LDAP directory Connection will only appear in the **Call Control** section.

For the scenario that the UC system has an LDAP connector and the user avatar photos only exist in the LDAP, (i.e. there are no user photos uploaded in UC), the LDAP picture will only appear in Call Control (WebClient and Fusion). The user photo will also appear in Call History , but will not keep appearing after you restart the client.

NOTICE:

This configuration is set by default in order to prevent picture requests to flood the LDAP server.

If you wish your avatar picture to appear in other sections as well or keep appearing after restarting the client and in the **Call History** , etc, it is recommended to import the pictures directly on the UC client. One option for configuring your UC avatar picture, is through **User Management**.

For more information please refer to the corresponding documentation.

6.10 UC Rapidstat Overview

The UC Rapidstat service allows the collection of various system data, generates alarms in case any problems are discovered and prints for V7 systems onwards an html report with all the collected data, including any warnings, errors or alarms.

NOTICE: UC Rapidstat is backwards compatible and allows you to download any V6 Rapidstat Report in a text file.

UC Rapidstat can run manually or automatically scheduled on a daily or weekly basis.

IMPORTANT: It is recommended that you run Rapidstat before any upgrade/migrate process takes place.

The information on how to display the report and what can be found in the Reports reside in the following sub-chapters:

[How to Add an LDAP Directory Connection](#) on page 401

[UC Rapidstat Report Text file](#) on page 418

6.10.1 UC Rapidstat Report in HTML

From V7 onwards Rapidstat report contains the following information in an html file which is stored and can be downloaded on request or/and can be displayed:

- **Deployment Type**

Rapidstat finds the current deployment scenario. Possible deployments are:

- Integrated Simplex
- Standard Duplex – Small Deployment
- Standard Duplex – Large Deployment
- Standard Duplex –Very Large Deployment

- **Rapidstat Alarms Information**

All alarms generated by this report are displayed in this section with their ID, Priority, Title, Description.

- **Host Name and IP address** per node is displayed in the header of the Rapidstat Node Information section.

- **Hardware Information**

Following hardware info is displayed: CPU, Physical Memory, Swap Memory (Used, Free, Buffers), Storage, Disks, Partitions, CD-ROMs, Network Cards, Network Interface, BIOS, Bridges.

- **Network Information**

- DNS Server (IP address)
- NTP Server (IP Address or hostname)
- Network Interfaces

All interfaces are listed and for every interface the following info is reported:

- 1) Name
- 2) Details
- 3) Auto-negotiation with info:

Supported (Yes/No)

Advertised (Yes/No)

Status (on/off)

NOTICE: If there is a DNS Server or NTP Server configured but no responding then a Minor Alarm is generated.

- **CPU Usage**

Rapidstat checks for processes taking up more than 90% of the CPU, which may be an indication to the user/administrator that those processes are not responding. This check is performed for every node.

- **Partitions**

The following partition information is displayed:

- Partition **Name**
- **Available space**
- **Used Space**
- **Used Space Percentage**

Rapidstat finds the physical partitions of every node and checks their used space percentage against the thresholds defined in the partitions configuration file, generating a minor, a major or a critical alarm if necessary.

The alarm, with information on the Partition Name and Alarm priority appears in the Partitions section and in the Rapidstat Alarms Information section.

NOTICE: An LVM snapshot may exist during backup and usage of syncUC, but it should not be older than hours since it heavily reduces system performance. So existence and age of the snapshot is displayed in this section of Rapidstat report. A snapshot older than 2 hours shall raise a critical alarm and a line will indicate a critical problem (snapshot run out of disc space).

- **Logical Volumes Information**

Following information about the existing logical volumes is displayed for each node:

- **Name** (Logical volume file path)
- Logical Volume **status**

- **Software Information**

Following information is displayed:

- **Operating System** (Linux version)
- **OpenScape UC** (Version, Release, Build)

- **Symphonia Processes status**

Rapidstat checks the status (i.e. running, unused, dead) of the following Symphonia Processes for every node.

- FrameworkContainer
- NotificationManager
- ActiveMQ
- TomcatServletContainer
- UDPForwarder
- WebClient_COMBINED

If any of the Symphonia Processes is not running a major Alarm is generated.

- **Virtual Machine Information**

If this is a Virtual Installation then you must install VMware tools to view details about this virtual machine.

- **Java VM Information**

This section displays the following information on JVM:

- JVM Memory (Heap and Non-Heap) statistics
- JVM Thread statistics
- various OpenSOAFramework MBeans

- **Symphonia JMX counters Information**

This section displays the following information on JVM:

- OpenSOAFramework MBeans
- OpenSOAFramework Contact Service

Counter **LDAPOverloadHit** for systems without problems must be =0.

NOTICE: The overload limit (default is 10) describes the max concurrent request allowed for each LDAP connector. Requests beyond are rejected. Therefore if the overload limit is reached it indicates performance problems of the LDAP connector

- **Partition Synchronization Information**

Rapidstat queries the status of syncUC partitioning, in order to find which syncUC partitions are active.

- **File access**

Existence and write access to directories and files is verified.

If there are any non writable file or missing files the log report path is displayed and a major alarm is generated.

- **Database Information**

This section displays the following on Database Information:

- Version

Displays the version of the currently installed database

- Status (Running or Stopped)

- Database Files (amount of DB found)

- Database Error Files (displays a list of all Error files with their full path name)

- Tables

Finds all the database tables that their number of rows exceed the threshold defined in the database configuration file.

- Database schema validity

Rapidstat validates database structure to ensure it's properly configured if there are any differences they shall be printed to stdout and stored in CheckSchema.log file. A minor alarm is generated and a message also appears in this field.

- CheckSchema.log timestamp

If it is available Rapidstat shall display timestamp of the checkSchema file, if it is not available a message appears recommending to launch persistence.checkSchema manually

- Database properties

- **System.xml Information**

Displays the following information on the System

- System data

- System Properties (address details and Company name)

- Node list (a list of all internal and external nodes displaying among others their guid, name, type, ip address, port)

- **Reachability and node IP resolve Information**

This section lists the information about the reachability status of each partner node.

- **Additional Information**

- ContactService Measure Time

Rapidstat measures the contact service response times in msecs.

NOTICE: The response time will be that of the slowest connector unless you configure the contact service

interface findContactByNumber to address each connector separately.

- CSTA Links Reachability (false or true)
- OpenScape Voice Compatibility

The Report lists all OSV nodes of the deployment with the following info:

1) Name

2) Reachability (A Node can be reachable or unreachable). A Major alarm is generated if the Node is unreachable.

3) Compatibility

Displays the compatibility status between the OSV Assistant and OSV switch for each switch, following values might appear:

`fully_compatible`= Assistant version is equal or higher than the OSV switch version.

`higher_version`= OSV switch version is higher than the Assistant version.

`lower_version`= Assistant version is much higher than OSV version.

NOTICE: The `lower_version` value may cause problems so the service personnel have to be aware of this situation.

4) no_compatibility = Assistant version is not compatible to OSV version. A Major alarm is generated for this value.

– **Network Communication Information**

This field displays the connectivity status to ports 4708-4711 and 7800.

– **OSGi.err and dump files information**

Rapidstat displays in this field the amount of the currently existing osgi.err files and dump files on every node. Details of these files can be found in the following paths:

`/var/siemens/common/log` for the `osgi.err` files

`/var/siemens/common/log/dumps` for the dump files

- **Appendix A: UC Licenses Details**

Rapidstat finds all OpenScape UC Application Licenses and reports the number of used Licenses (used licenses/total amount of license)

- **Appendix B: Number of UC Users**

Rapidstat finds the total amount of Users with a UC profile.

6.10.2 UC Rapidstat Report Text file

Rapidstat reports generated in V6 contain the following information in a text file which is stored and can be downloaded on request:

- **DEPLOYMENT**

Rapidstat finds the current deployment scenario. Possible deployments are:

- Integrated Simplex
- Standard Duplex – Small Deployment
- Standard Duplex – Large Deployment

- **DATABASE VERSION**

Rapidstat finds the version of the currently installed database.

- **DATABASE STATUS**

Rapidstat finds the status (Running or Stopped) of the database.

- **DATABASE FILE SIZE**

Rapidstat finds the database files and checks their size against the thresholds defined in the database configuration file, generating a minor or a major alarm if necessary.

- **DATABASE ERROR LOG**

Rapidstat checks if the database error log file exists (e.g. for Solid database, it checks for the existence of solerror.out) and generates a minor alarm in case the file did not exist or has changed since last execution.

- **NUMBER OF ROWS OF DATABASE TABLES**

Finds all the database tables that their number of rows exceed the threshold defined in the database configuration file.

- **STATUS OF PARTITION SYNCHRONIZATION**

Rapidstat queries the status of syncUC partitioning, in order to find which syncUC partitions are active.

- **DUMP FILES**

Rapidstat makes a list of the currently existing dump files (e.g Java core dump files) on every node.

- **INSTALLED HARDWARE**

Rapidstat finds for every node the installed hardware, such as CPUs, Hard disks, Network cards, etc

- **MEMORY USAGE**

Rapidstat gathers data regarding physical and swap memory, such as free and used memory.

- **CPU USAGE**

Rapidstat checks for processes taking up more than 90% of the CPU, which may be an indication to the user/administrator that those processes are not responding. This check is performed for every node.

- **NETWORK SETTINGS**

Rapidstat finds the network settings of every node. Those settings include the DNS servers, the NTP server and the list of network interfaces.

- **OSGi ERROR FILES**

Rapidstat makes a list of the currently existing osgi.err files on every node, displaying the contents (i.e. error messages) of each osgi.err file.

- **PARTITIONS OF EVERY NODE**

Rapidstat finds the physical partitions of every node and checks their used space percentage against the thresholds defined in the partitions configuration file, generating a minor or a major alarm if necessary.

- **INSTALLED SOFTWARE**
Rapidstat finds for every node the version of the installed operating system and the version of the installed OpenScapeUC.
- **SYMPHONIA PROCESSES STATUS**
Rapidstat checks the status (i.e. running, unused, dead) of the Symphonia Processes for every node.
- **JVM STATISTICS**
Rapidstat queries the JVM it runs on, regarding JVM Memory (Heap and Non-Heap) statistics, JVM Thread statistics and various OpenSOAFramework MBeans.
- **UC LICENSES**
Rapidstat finds all OpenScape UC Application Licenses and reports the number of used Licenses (used licenses/total amount of license)
- **UC Users**
Rapidstat finds the total amount of Users with a UC profile.

6.10.3 How to Display UC Rapidstat

You can run a UC Rapidstat report manually or automatically on a daily or weekly basis.

Prerequisites

- Adequate administrative permissions
- You have deployed Unified Communications in one of the following configurations:
 - Integrated Deployment
 - Small Deployment
 - Large Deployment
 - Very Large Deployment

Step by Step

- 1) On the **Maintenance** navigation tab, click on the Inventory navigation menu item.
- 2) In the navigation tree, click on **Nodes&Applications > Nodes**.
A list of all system nodes and 3rd party system connections available in the entire system is displayed in the work area.
- 3) Click on the name of the system node the dashboard of which you want to display.
 - a) For an Integrated Simplex click on the communication node
 - b) For a Small or Large Deployment click on the Application Server node (Default node name is Offboard)A dialog with the dashboard of the selected system node opens.
- 4) Navigate to Actions area and click on **Show** button next to UC Rapidstat
The Rapidstat window opens. The information area displays the UC Rapidstat scheduled frequency (daily or weekly) and the last run date.

- 5) Click on the **Start** button to initiate manually a Rapidstat Report

This job might take a few seconds and you are requested to wait until the job is completed.

The Rapidstat Report file is produced with a file name containing the time stamp of creation down to the second:
RapidstatReport_yyyymmddHHMMSS.html

The Rapidstat Report is an html file and is added at the end of available reports list and can be downloaded.

NOTICE: It is advised to initiate a Rapidstat report outside business hours

- 6) You can select a report from the pull down menu and click one of the available buttons:

a) **Download**

You are prompted to save the report file.

NOTICE:

The report file can either be an html if generated in V7 or you can have in the download list txt files generated by Rapidstat in a V6 UC deployment.

b) **Show**

The UC Rapidstat Report is displayed in html format.

- 7) Click on **Configure** button to configure the scheduled report as described in the relevant chapter.
- 8) Click on the **Close** button to close the window.

6.10.4 How to Configure UC Rapidstat Settings

You can configure the report schedule, the log history settings , the thresholds for Database File sizes and Hard disc space allocation for UC Rapidstat service.

Prerequisites

- Adequate administrative permissions
- You have deployed Unified Communications in one of the following configurations:
 - Integrated Deployment
 - Small Deployment
 - Large Deployment
 - Very Large Deployment

Step by Step

- 1) On the **Maintenance** navigation tab, click on the Inventory navigation menu item.

- 2) In the navigation tree, click on **Nodes&Applications > Nodes**.
A list of all system nodes and 3rd party system connections available in the entire system is displayed in the work area.

- 3) Click on the name of the system node the dashboard of which you want to display.
 - a) For an Integrated Simplex click on the Communication systems node.
 - b) For a Small or Large Deployment click on the Application Server node (Default node name is Offboard).

A dialog with the dashboard of the selected system node opens.

- 4) Navigate to Actions area and click on Show button next to UC Rapidstat.
The Rapidstat window opens. The information area displays the UC Rapidstat scheduled frequency (daily or weekly) and the last run date.

- 5) Click on the **Configuration** button.

The Rapidstat Settings window opens

- 6) Configure the report frequency by choosing one of the following values next to the **Run every** field:

Week

Day

disable (if you choose this value UC Rapidstat report can only be generated manually)

- 7) Enter the time and day you want the UC Rapidstat to run.

NOTICE:

It is advised that you schedule UC Rapidstat to run outside business hours

- 8) Select the amount of times you want UC Rapidstat to run from **Occurrences** field:
infinitely (Rapidstat will run according to the schedule until you change this value)
finite number of times (if you choose this value you must also enter the number times you want UC Rapidstat to run)
- 9) In the **Log history** field (default value is 10) enter the maximum amount of report files you want UC Rapidstat to keep stored.

IMPORTANT: If maximum amount of files is reached then at the end of each run of RapidStat service the new file will be saved and older file which exceeds the configured number of report files shall be deleted.

- 10) Navigate to the Database file size section.

- 11) Set the database file size threshold in MB that will trigger the following alarms:
- **Minor Alarm** (default values are 80000MB for Small/Large Deployment, 1600MB for Integrated Simplex)
 - **Major Alarm** (default values are 90000MB for Small/Large Deployment, 1800MB for Integrated Simplex)
 - **Critical Alarm** (default values are 95000MB for Small/Large Deployment, 1900MB for Integrated Simplex)

NOTICE: If you want to switch off completely the Hard disc percentage alarms, you have set 0 value to all three of them.

IMPORTANT: Configuration of HD Space allocation values affects all nodes. Individual or partition specific settings must be performed manually as described in the relative chapter "How to Configure manually the partition specific settings for UC Rapidstat xml files"

6.10.5 How to Configure manually the partition specific settings for UC Rapidstat xml files

The administrator can configure manually the partition specific settings for UC Rapidstat xml files.

Prerequisites

- Adequate administrative permissions
- You have deployed Unified Communications in one of the following configurations:
 - Integrated Deployment
 - Small Deployment
 - Large Deployment
 - Very Large Deployment

Step by Step

- 1) Open Partitions configuration file from following path:

For an Integrated Simplex deployment:

`/enterprise/common/conf/rapidstat_partitions.xml`

For an Small or Large deployment an instance of this file resides on every node (i.e. Backend, Frontend, Media Server) so you need to configure it for every node in the path:

`/opt/siemens/common/conf/rapidstat_partitions.xml`

The xml file opens.

2) Following parameters are configured in the rapidstat_partitions.xml file:

- Name: The particular partition that the entry applies to. (e.g. /dev/sda2)

Entry with default value is applied to all partitions.

- UsedSpacePercentageMinorAlarm: the percentage (%) of used disk space; if this threshold is exceeded by any partition, a minor alarm will be generated.

- UsedSpacePercentageMajorAlarm: the percentage (%) of used disk space; if this threshold is exceeded by any partition, a major alarm will be generated.

- UsedSpacePercentageCriticalAlarm: the percentage (%) of used disk space; if this threshold is exceeded by any partition, a critical alarm will be generated.

The initial entry of the xml file is the default partition with the following default values for all deployment except for Integrated Simplex:

80 % for UsedSpacePercentageMinorAlarm

90 % for UsedSpacePercentageMajorAlarm

95 % for UsedSpacePercentageCriticalAlarm

The following are the default values for **Integrated Simplex**:

60 % for UsedSpacePercentageMinorAlarm

70 % for UsedSpacePercentageMajorAlarm

80 % for UsedSpacePercentageCriticalAlarm

IMPORTANT: There must ALWAYS be a default partition entry in the rapidstat_partitions.xml file.

You might find useful the following additional entries in the rapidstat_partitions.xml file:

You can switch off completely the feature that checks the used space for every partition and generates alarms by setting the following values

```
Name= default
UsedSpacePercentageMinorAlarm=0
UsedSpacePercentageMajorAlarm=0
UsedSpacePercentageCriticalAlarm=0
```

NOTICE: This can also be configured in the relevant UI page Rapidstat Configuration.

You can define different alarm levels than the default ones for a particular partition (e.g. /dev/sda2), by adding an entry with the following values:

```
Name = /dev/sda2
UsedSpacePercentageMinorAlarm =60
UsedSpacePercentageMajorAlarm =75
```

```
UsedSpacePercentageCriticalAlarm =80
```

You can exclude a particular partition (e.g. /dev/sda3) from the check for used space and the generation of alarms, by adding an entry with the following values:

```
Name = /dev/sda3
UsedSpacePercentageMinorAlarm =0
UsedSpacePercentageMajorAlarm =0
UsedSpacePercentageCriticalAlarm =0
```

- 3) Save the file `rapidstat_partitions.xml` in the directory you initially retrieved it from.

6.11 Managing Groupware Services

This chapter provides information about the following topics:

General groupware service information

- [Groupware Service Concept](#)
- [Adding a Groupware Connection](#)
- [Displaying a Groupware Connection](#)

Information related to IBM Lotus Notes

- [Displaying / Editing Groupware-Domino Connector Settings](#)
- [Displaying / Editing the IBM Lotus Notes System Configuration](#)

Information related to Microsoft Exchange

- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#)
- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#)
- [Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP](#)
- [Configuring the encrypted Transmission between Groupware-Exchange Connector and Microsoft Exchange Servers](#)

Groupware service information independent from groupware

- [Displaying / Editing Settings for an independent SMTP Server Connection](#)
- [Configuring the Contact Data Replication of the Groupware Service](#)
- [Configuring restricted Access to private Groupware Contacts](#)

6.11.1 Groupware Service Concept

You use the groupware service to connect the OpenScape system with one of the following external groupware systems.

- IBM Lotus Domino 8.5.x Server IBM Lotus Domino 9.0.x Server Microsoft Exchange Server 2013 Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

In case of such a connection the groupware service controls access to mail data, calendar data and contact data of the relevant OpenScape users.

Connecting an external groupware system to the OpenScape system via the groupware service has the following advantages for OpenScape users:

- Voice messages are stored in the groupware inbox of the addressed OpenScape user.
- OpenScape users may access their groupware inboxes via the voice portal and perform the following tasks:
 - Playing /deleting /restoring messages
 - Marking messages as read/unread.
 - Answering/forwarding messages with a voicemail
 - Creating new voicemails
- OpenScape users may access their groupware calendars via the voice portal and perform the following tasks:
 - Playing / accepting /declining appointments
 - Sending a voicemail to the appointment initiator
- OpenScape users can deploy their OpenScape Web Client or OpenScape Desktop Client to access their groupware contacts and perform the following tasks:
 - Creating /deleting /modifying/searching for contacts

Specials for connecting Microsoft Exchange

You can connect the groupware service to Microsoft Exchange in two ways:

- For Microsoft Exchange 2013, 2016 or 2019 via Web Services.

NOTICE: For configuring a Groupware connection with deprecated "WebDAV connection type" you may refer to UC V9 Official documentation.

In operation, OpenScape UC Application creates independently e-mails and sends them to the e-mail inboxes of the Microsoft Exchange server. The groupware service sends such anonymous e-mails via an SMTP server, which forwards them accordingly.

A groupware service entity can always connect only one groupware server to the OpenScape system.

If the groupware service connects an Microsoft Exchange server, it cannot access the server's global address list (GAL).

The groupware service can be configured for a Microsoft Exchange server in such a way that OpenScape users are given read-only access to their private Microsoft Exchange contacts.

Specials for connecting IBM Lotus Domino

The groupware service does not directly access the user data of the productive IBM Lotus Domino servers (groupware servers). Instead, it accesses a Notes API, which you install on the OpenScape UC Application computer system with an IBM Lotus Domino server (connector server). This Notes API then uses a technical user account to connect to the groupware server.

- A groupware service entity can always connect only one IBM Lotus Domino server to the OpenScape system.
- If the groupware service connects to an IBM Lotus Domino server, it cannot access databases exclusively locally stored in a Lotus Notes client.

Specials without a Microsoft Exchange or IBM Lotus Domino connection

If no groupware system is connected to OpenScape UC Application, you can connect OpenScape UC Application to an independent SMTP server. OpenScape UC Application then sends e. g. all automatically created notifications via this SMTP server, inclusive those for the Tell-me-when feature.

6.11.2 Adding a Groupware Connection

How to add a new groupware connection:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select **Add**.

The dialog for adding a new groupware connection opens.

- 5) Select under **Connection Type** the desired type of groupware connection.

You can choose from:

- **Lotus Notes** for connecting an IBM Lotus Domino server.
- **Microsoft Exchange Web Services** For connecting a Microsoft Exchange server 2013, 2016 or 2019.
- **SMTP** For connecting an independent SMTP server if neither an IBM Lotus Domino nor a Microsoft Exchange server is connected to OpenScape UC Application.

NOTICE: If you configure a groupware connection of type **Lotus Notes** or **Microsoft Exchange Web Services**, you cannot create a second groupware connection.

- 6) Specify a unique identifier for the connection under **Connection ID**.

Example: ConnectionMSE2003

In case of a Microsoft Exchange or IBM Lotus Domino connection, this identifier is used to assign this connection to OpenScape users.

- 7) Select **Save**.

The new connection is displayed in the list of all configured groupware connections.

- 8) Configure the groupware connector appropriate for the groupware connection.

You find detailed information about the groupware connection settings that depend on connectors under:

- [Displaying / Editing Groupware-Domino Connector Settings](#) on page 428
- [Displaying / Editing the IBM Lotus Notes System Configuration](#) on page 429
- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#) on page 431
- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#) on page 431
- [Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP](#) on page 433
- [Displaying / Editing Settings for an independent SMTP Server Connection](#) on page 439

6.11.3 Displaying a Groupware Connection

How to display or modify the settings of a groupware connection:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.

You find detailed information about the groupware connection settings that depend on connectors under:

- [Displaying / Editing Groupware-Domino Connector Settings](#) on page 428
- [Displaying / Editing the IBM Lotus Notes System Configuration](#) on page 429
- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#) on page 431
- [Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services](#) on page 431
- [Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP](#) on page 433
- [Displaying / Editing Settings for an independent SMTP Server Connection](#) on page 439

6.11.4 Displaying / Editing Groupware-Domino Connector Settings

How to display or modify the Groupware-Domino connector settings:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select the radio button of the IBM Lotus Notes connection the settings of which you want to display or edit.
- 5) Select **Configure**.

The dialog with the Groupware-Domino connector settings opens.

You see the following data:

Connection Type Specifies the groupware connection type. **Lotus Notes** is displayed for an IBM Lotus Domino connection.

Connection ID Unique identifier for the IBM Lotus Domino connection. This identifier is used for assigning this connection to OpenScape users.

Furthermore, you can change the following data:

Description A short description of the groupware connection.

Domino Directory Server Name of an IBM Lotus Domino directory server. You need to specify this name in canonical notation.

Example: CN=Domino/OU=Doc/O=Org/C=DE

Default Sender Address Is usually the e-mail address of the technical user account. This address is used as originator address for e-mails that OpenScape UC Application sends automatically. OpenScape UC Application sends non-delivery reports to this address also.

- 6) Select **Save** to copy the modified settings.

6.11.5 Displaying / Editing the IBM Lotus Notes System Configuration

How to display or modify the IBM Lotus Domino connector server configuration:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

3) Switch to the **Lotus Notes System Configuration** tab.

You see the following data:

Active Lotus Notes User ID Specifies the IBM Lotus Notes user ID currently used for the IBM Lotus Domino connection. This is the ID file of the technical user account. The ID is displayed in canonical notation.

Furthermore, you can change the following data:

Lotus Notes ID File Name of the ID file to be used instead of the currently active ID file. For activating a specified ID file you need to select **Change User ID** after choosing the file.

Password Password for the technical user account. For activating a modified setting in this field you need to select **Change User ID** after the modification.

Change User ID Activates modified settings in the **Lotus Notes ID File** and **Password** fields.

Domino Server Connections Should display all IBM Lotus Domino servers on which mail databases are managed. The IBM Lotus Domino directory server specified on the **Connection Configuration** tab must also be present. You need to select **Activate Server Connections** for using modified Domino server connections.

4) Select **Add** for adding a new Domino server connection.

A new entry is added to the connection list. You need to perform the following settings for this entry:

- **Domino Server Name**

Name of the relevant IBM Lotus Domino server in hierarchical notation.

Example: dominoServer1/orgUnit1/Org1

NOTICE: You can look for the server name in the Domino directory.

- **Domino Server Address**

IP address of the computer system that hosts the specified IBM Lotus Domino server.

If the host name of the computer system can be resolved into an IP address via a DNS server, you can also enter the associated host name instead of the IP address.

5) For changing a setting, click in the relevant field of a Domino server connection and perform the modification.

6) For deleting a Domino server connection select the relevant list entry and click on **Remove**.

7) After you have changed the settings of the Domino server connection click on **Activate Server Connections** for applying the performed settings to the connector server.

6.11.6 Displaying / Editing Settings of the Groupware-Exchange Connector for Web Services

NOTICE: This Groupware-Exchange connector is used for connecting a Microsoft Exchange 2013 / 2016 / 2019.

How to display or modify the Groupware-Exchange connector settings for Web Services:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select the radio button of the Microsoft Exchange Web Services connection the Web Services settings of which you want to display or edit.
- 5) Select **Configure**.

The dialog with the Groupware-Exchange connector settings for Web Services opens.

The **Exchange Web Services Configuration** tab displays the following data:

Connection Type Specifies the groupware connection type. **Microsoft Exchange Web Services** is displayed for a Microsoft Exchange Web Services connection.

Connection ID Unique identifier for the Microsoft Exchange Web Services connection. This identifier is used for assigning this connection to OpenScape users.

- 6) Specify under **Domain** the name of the Windows domain that hosts the Microsoft Exchange server.

In doing so use the NetBIOS name.

Example:

Domain name fully qualified:	EXCH.unify.com
Domain name NetBIOS:	EXCH

- 7) Enter the name of the technical user account in the **Technical User Account** field.
- 8) Enter the password of the technical user account in the **Password** field.

NOTICE: The Groupware-Exchange connector attempts to log on to the Microsoft Exchange server with the following authentication processes in the given sequence: – BASIC – DIGEST – NTLM

NOTICE: Using NTLM v2 requires performing the following in the EWS settings of Microsoft Exchange: –

Authentication processes BASIC and DIGEST disabled
– Windows authentication active (default setting) –
Anonymous authentication as is default in the EWS settings
You find information about the Microsoft Exchange default settings depending on the version for example under the following links: Microsoft Exchange Server 2013: <https://docs.microsoft.com/en-us/exchange/default-settings-for-exchange-virtual-directories-exchange-2013-help> Microsoft Exchange Server 2016/2019: <https://docs.microsoft.com/en-us/exchange/clients/default-virtual-directory-settings?view=exchserver-2019>

- 9) Select one of the following options under **Exchange Access Mode**:
- **Manual Configuration** for configuring a static URL for accessing the Web Services interface.
 - **Static Autodiscovery** for activating the static mode of Autodiscover.
 - **Dynamic Autodiscovery** for activating the dynamic mode of Autodiscover.

NOTICE: We recommend to always use dynamic Autodiscover.

NOTICE: You find technical information about Autodiscover in [Configuring the Autodiscover Service for Microsoft Exchange 2013 / 2016 / 2019](#).

- 10) If you have selected the **Manual Configuration** option under **Exchange Access Mode**:

Enter under **Exchange Web Services URL** the static address for accessing the Web Services interface.

Example of unencrypted communication: `http://10.10.1.1./ews/exchange.asmx`

Example of SSL-based encrypted communication:
`https://10.10.1.1./ews/exchange.asmx`

NOTICE: The specified address must be resolvable in the network – e. g. via a corresponding DNS entry.

NOTICE: For using SSL you need to copy the SSL certificate of the OWA server to the OpenScape keystore. How to proceed is described in [Configuring the encrypted Transmission between Groupware-Exchange Connector and Microsoft Exchange Servers](#) on page 435.

- 11) If you have selected the **Static Autodiscovery** option under **Exchange Access Mode**:

Specify under **Autodiscover URL** the static address for the Groupware-Exchange connector to send Autodiscover requests to.

Example: `https://exchange.domain154`

NOTICE: The specified address must be resolvable in the network – e. g. via a corresponding DNS entry.

- 12) If you have selected the **Dynamic Autodiscovery** option under **Exchange Access Mode**:

Specify under **Autodiscover URL Prefix** the prefix from which the dynamic URL shall be created for the Autodiscover service.

Example: `autodiscover`

NOTICE: Depending on the Microsoft Exchange organization configuration you probably need not make an entry in this field.

NOTICE: Verify that all addresses of the following format are resolvable in the network – e. g. via a corresponding DNS entry. `https://<prefix>.<SMTP domain>/autodiscover/autodiscover.xml`

- 13) If you have selected one of the Autodiscover options under **Exchange Access Mode**:

Select one of the following options under **Autodiscover Protocol**:

- **Internal** if OpenScape UC Application can reach the URLs of all Web Services within a corporate network without firewall transitions.
- **External** if OpenScape UC Application can reach the Web Services URLs via firewall barriers only.

- 14) To test the Microsoft Exchange connection at a later date, enter a primary e-mail address under **Primary Emailaddress of the Test Mailbox**. This primary address must be available as valid address in one of the connected Microsoft Exchange servers.

NOTICE: The specified address is only used to test the Microsoft Exchange connection functionality.

- 15) Select **Save** to copy the modified settings.

You find details of the settings on the **SMTP Configuration** tab in [Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP](#) on page 433.

6.11.7 Displaying / Editing Settings of the Groupware-Exchange Connector for SMTP

How to display or modify the SMTP settings of the Groupware-Exchange connector for Web Services:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.
The groupware configuration dialog opens.
- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select the radio button of the Exchange Web Services connection the SMTP settings of which you want to display or edit.
- 5) Select **Configure**.

The dialog with the Groupware-Exchange connector settings opens.

- 6) Switch to the **SMTP Configuration** tab.

On this tab you can change the following data:

Default Sender Address Is usually the e-mail address of the technical user account. This address is used as originator address for e-mails that OpenScape UC Application automatically sends via the SMTP server of the Microsoft Exchange server – thus for voice messages left via the voice portal's guest access. OpenScape UC Application sends non-delivery reports to this address also.

NOTICE: Please note the following for voice messages left by callers e.g. in the voice portal's guest access and sent to the relevant OpenScape users as e-mail: If the Microsoft Exchange server can resolve the deployed technical user account in a display name, the inbox displays for the associated e-mail the mailbox name of the technical user account as originator address and not the originator number of the caller.

SMTP Host IP address under which the SMTP server of the Microsoft Exchange server can be reached. If your network has a Domain Name Service (DNS), you can also specify the host name of the associated computer system as alternative.

Port Port the Groupware-Exchange connector is to use for the SMTP communication. This is port **25 by default**.

Enable STARTTLS Activates the option of communicating with the SMTP server via TLS.

NOTICE: A STARTTLS-based connection always starts unencrypted and switches to TLS only if TLS is active for both communication partners.

Enable Authentication Activates the authentication for communicating with the SMTP server. With authentication being active you need to specify

access data under **User Name** and **Password** that the Groupware-Exchange connector can use for accessing the SMTP server.

NOTICE: The Groupware-Exchange connector attempts to log on to the Microsoft Exchange server with the following authentication processes in the given sequence: – BASIC – DIGEST – NTLM

NOTICE: Using NTLM v2 requires performing the following in the EWS settings of Microsoft Exchange: – Authentication processes BASIC and DIGEST disabled – Windows authentication active (default setting) – Anonymous authentication as is default in the EWS settings You find information about the Microsoft Exchange default settings depending on the version for example under the following links: Microsoft Exchange Server 2013: <https://docs.microsoft.com/en-us/exchange/default-settings-for-exchange-virtual-directories-exchange-2013-help> Microsoft Exchange Server 2016/2019: <https://docs.microsoft.com/en-us/exchange/clients/default-virtual-directory-settings?view=exchserver-2019>

7) Select **Save** to copy the modified settings.

6.11.8 Configuring the encrypted Transmission between Groupware-Exchange Connector and Microsoft Exchange Servers

In case of a Microsoft Exchange connection, information can be transmitted between Groupware-Exchange connector and Microsoft Exchange servers securely. The Groupware-Exchange connector supports the following protocols for this purpose by default:

- Web-services-based connection the protocol TLS 1.0.

How to activate encryption for the communication between Groupware-Exchange connector and Microsoft Exchange organization:

- 1) [Loading Certificates from the Microsoft Exchange Servers](#)
- 2) [Importing Certificates in OpenScape UC Application](#)
- 3) [Activating the Encryption](#)

These steps are described in detail in the following sections.

6.11.8.1 Loading Certificates from the Microsoft Exchange Servers

If the Groupware-Exchange connector is to communicate with the systems of the Microsoft Exchange organization securely, certificates must exist for the host part of all of the following URLs depending on the configuration ¹⁹. This

¹⁹ If there are several different URLs for the same host, merely one certificate is required in total.

may require several different host-individual certificates or a common SAN-certificate²⁰ for all relevant hosts.

- **If you use a web-services-based connection without Autodiscover:**
 - For the Web Services URL used.
- **If you use a web-services-based connection with static Autodiscover:**
 - For the Autodiscover URL used.
 - For all Web Services URLs that can be published by the addressed CAS upon Autodiscover requests.
- **If you use a web-services-based connection with dynamic Autodiscover:**
 - For all Autodiscover URLs that can be dynamically created by the Groupware-Exchange connector.
 - For all Web Services URLs that can be published by all possibly addressed CAS upon Autodiscover requests.

All certificates used must be made known to the Groupware-Exchange connector by importing the keys in the groupware keystore of OpenScape UC Application. To do this, they must be previously downloaded from the associated computer systems.

NOTICE: The following description assumes that the Microsoft Exchange certificate is recognized as valid certificate by the web browser used. The root certificate with which the Microsoft Exchange certificate was signed must have already been imported in the web browser used. The same applies to intermediate certificates that the web browser may need to recognize the Microsoft Exchange certificate. Whether or not a certificate is recognized as valid

is displayed to you e.g. in the Internet Explorer by the



icon.

Start the configuration

How to load the certificates of the relevant Microsoft Exchange servers:

- 1) Open your web browser and invoke the following address of a relevant Microsoft Exchange server:

Example of the Web Services URL: `https://<IP address/FQDN>/ews/exchange.asmx`

Example of the Autodiscover URL: `https://<IP address/FQDN>/autodiscover/autodiscover.xml`

Replace `<IP address/FQDN>` with the IP address or the fully qualified host name under which the relevant Microsoft Exchange server can be reached.

- 2) Authenticate with the user data of the technical user who you also use for the Microsoft Exchange connection.
- 3) If a certificate is offered to you for confirmation, accept it.

²⁰ SAN certificates are not only issued for a single fully qualified host name but for several host names.

- 4) Export the certificate of the relevant Microsoft Exchange server as CER file.

How to proceed in the Internet Explorer for example:

- a) Select in the main menu **Tools > Internet Options....**
- b) Switch to the **Content** tab.
- c) Select **Certificates**.

A window with all stored certificates opens.

- d) Search the available tabs for the certificate of the relevant Microsoft Exchange server and select it.
- e) Select **Export**.

The certificate export wizard opens.

- f) Follow the wizard and export the certificate with the **Base-64-coded X.509 (.CER)** option.

You have now loaded the certificate of the relevant Microsoft Exchange server.

- 5) Execute steps 1 to 4 for all relevant Microsoft Exchange servers, so that eventually each required certificate is available as CER file.

You have now loaded all required certificates.

6.11.8.2 Importing Certificates in OpenScape UC Application

So that the Groupware-Exchange connector can use the public keys of the certificates for encryption, you must import the certificates in the groupware keystore of OpenScape UC Application.

Start the configuration

How to import the certificates in the groupware keystore:

- 1) Copy all of the just loaded CER files to the application computer of OpenScape UC Application.
- 2) Open a shell on the application computer and switch to the directory in which the Java keytool is installed.

[Determining the Keytool Command](#) describes how to determine this directory.

- 3) Execute the following lines as one command in the relevant directory for each CER file:

```
keytool -import -file <storage location and name of the CER file> -  
keystore <Osc-Install21>/scs_groupware/conf/groupware.jks -storepass  
grppasswd
```

- 4) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 5) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 6) Select the radio button of the Microsoft Exchange connection.
- 7) Select **Configure**.

The configuration dialog of the selected connection opens.

²¹ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

- 8) Click on **Save** to copy the settings for the Groupware-Exchange connector unchanged once more.

The Groupware-Exchange connector now adopts the public keys of the certificates.

- 9) Symphonia restart is required after importing the certificate to the groupware keystore

6.11.8.3 Activating the Encryption

So that the Groupware-Exchange connector communicates with the systems of the Microsoft Exchange organization securely, you need to activate the encryption in the Groupware-Exchange connector.

Start the configuration

How to activate the encryption in the Groupware-Exchange connector:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.

The groupware configuration dialog opens.

- 3) Select the radio button of the Microsoft Exchange connection.
- 4) Select **Configure**.

The configuration dialog of the selected connection opens.

- 5) Execute one of the following steps depending on the configuration used:

- **If you have connected the Microsoft Exchange organization via Web Services without Autodiscover:**

Specify under **Exchange Web Services URL** the HTTPS address under which the OWA server used can be reached.

Example: `https://10.10.1.1./ews/exchange.asmx`

- **If you have connected the Microsoft Exchange organization via Web Services with static Autodiscover:**

Specify under **Autodiscover URL** the HTTPS address under which the CAS server used can be reached.

Example: `https://exchange.domain154/autodiscover/autodiscover.xml`

- **If you have connected Microsoft Exchange via Web Services with dynamic Autodiscover:**

Dynamic Autodiscover uses encrypted communication exclusively. Consequently, you need not configure anything in the Groupware-Exchange connector.

- 6) Select **Save**.

The configuration dialog closes and the settings are saved.

You have now activated the encryption in the Groupware-Exchange connector.

From now on, information is transmitted between the Groupware-Exchange connector and the systems of the Microsoft Exchange organization securely.

6.11.9 Displaying / Editing Settings for an independent SMTP Server Connection

If no groupware system is connected to OpenScape UC Application, you must connect OpenScape UC Application to an independent SMTP server. OpenScape UC Application then sends e. g. all automatically created notifications via this SMTP server, inclusive those for the Tell-me-when feature.

How to display or modify the settings for connecting the independent SMTP server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Connections > Groupware**.
The groupware configuration dialog opens.
- 3) Verify that the **Connection Configuration** tab is displayed. On this tab you see all configured groupware connections.
- 4) Select the radio button for the connection to the independent SMTP server.
- 5) Select **Configure**.

The dialog with the settings of the independent SMTP server opens.

You see the following data:

Connection Type

Specifies the connection type. **SMTP** is displayed for the connection to an independent SMTP server.

Connection ID

Unique identifier for the connection.

Furthermore, you can change the following data:

Description

A short description of the connection to the independent SMTP server.

Default Sender Address

Specifies a valid e-mail address. This address is used as originator address for e-mails that OpenScape UC Application sends automatically via the external SMTP server – in particular also for voice messages left via the

voice portal's guest access. OpenScape UC Application sends non-delivery reports to this address also.

SMTP Host

IP address under which the independent SMTP server can be reached. If your network has a Domain Name Service (DNS), you can also specify the host name of the associated computer system as alternative.

Port

Port the SMTP connector is to use for the SMTP communication. This is port **25 by default**.

Enable STARTTLS

Activates the option of communicating with the SMTP server via TLS.

NOTICE: To use TLS, the certificate of the SMTP server must be imported in the groupware keystore of OpenScape UC Application. Proceed precisely as described in [Importing Certificates in OpenScape UC Application](#) on page 437.

NOTICE: A STARTTLS-based connection always starts unencrypted and switches to TLS only if TLS is active for both communication partners.

Enable Authentication Activates the authentication for communicating with the SMTP server. With authentication being active you need to specify access data under **Authentication Realm**, **User Name** and **Password** that the SMTP-Exchange connector can use for accessing the SMTP server.

NOTICE: The independent SMTP connector attempts to log on to the SMTP server with the following authentication processes in the given sequence:

- PLAIN
 - LOGIN
 - DIGEST
-

6) Select **Save** to copy the modified settings.

6.11.10 Configuring the Contact Data Replication of the Groupware Service

NOTICE: Because the Groupware-Domino connector is not supported for Very Large Deployment, you cannot configure the contact data replication with Lotus Domino for Very Large Deployment.

To access the groupware server as rarely as possible, the groupware service caches the private contact data of all users on the application computer of OpenScape UC Application. You can replicate the contact data stored in this way with the contact data in the groupware server in configurable intervals. The

content of the following configuration file determines when this contact data replication is performed.

gwlookup.quartz_jobs.xml

You find this file in the following directory on the application computer:

<Osc-Install²²>/scs_groupware/conf

In the configuration file you configure the settings for the following three replication jobs:

- **Data synchronization upon the initialization**

IMPORTANT: The configuration of this job must not be modified.

This job is described in the configuration file by the **initially** value in the **name** XML element.

- **Complete data synchronization**

This job replicates the cached contact data with all contact data of all users in the groupware server. This replication causes high data traffic. Therefore, execute this job at times of low payload – for example at night.

This job is described in the configuration file by the **fullUpdate** value in the **name** XML element.

- **Differential data synchronization**

This job replicates the cached contact data with all modified contact data of all users in the groupware server.

This job is described in the configuration file by the **differentialUpdate** value in the **name** XML element.

- While the initial database replication is always performed immediately after each new start of the application computer, you can determine yourself when the complete and differential data replication shall take place. A cron job is pre-configured as trigger for the complete and differential data replication.

To change the execution time for a cron job, you need to configure the value for the associated XML element **cron-expression**.

Example: <cron-expression>**0 43 0,3-23 * * ?**</start-time>

The value of **cron-expression** defines the following fields in the given sequence and separated by blanks:

- Seconds
- Minutes
- Hours
- Days of a month
- Month
- Days in a week
- Year (optional)

In the given example, a cron job would be executed every day at the following times: 00:43:00, 03:43:00, 4:43:00 ... 23:43:00.

²² <Osc-Install> is the setup directory of OpenScope UC Application: /opt/siemens/ respectively / enterprise/

You find a detailed description of the settings syntax under the following link:
<http://www.quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger>

Simple trigger

Instead of a pre-set cron job trigger you can also configure a simple trigger for the complete and differential data replication. Because the cron job trigger settings are more comprehensive, this trigger should be preferred.

The following settings exist for a simple trigger:

- **start-time**

This setting determines when the data replication is performed for the first time. You may only specify a past or future point in time.

Example:

```
<start-time>2008-4-22 1:00:00 AM</start-time>
```

IMPORTANT: You need to specify the time exactly in the format as shown in the example.

- **repeat-count**

This setting determines how often this job is repeated. Value -1 means that the job is repeated infinitely.

Example:

```
<repeat-count>-1</repeat-count>
```

- **repeat-interval**

This setting determines after which time the next job is started. The set value is interpreted in milliseconds.

Example of daily repetition:

```
<repeat-interval>86400000</repeat-interval>
```

Example of a simple trigger:

```
...
<job>
  <job-detail>

  ...
  </job-detail>
  <trigger>
    <simple>
      <name>fullTrigger</name>
      <group>DEFAULT</group>
      <job-name>fullUpdate</job-name>
      <job-group>DEFAULT</job-group>
      <start-time>2008-04-22 01:00:00</start-time>
      <repeat-count>0</repeat-count>
      <repeat-interval>1</repeat-interval>
    </simple>
  </trigger>
</job>
```

6.11.11 Configuring restricted Access to private Groupware Contacts

The groupware service can be configured for a Microsoft Exchange server in such a way that OpenScape users are given read-only access to their private Microsoft Exchange or IBM Lotus Domino contacts.

How to allow only read-access to the private groupware contacts for OpenScape users:

- 1) Select in the CMP toolbar in the **Domain** combo box the domain for the users of which you want to configure the contact access.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 3) In the navigation tree, click **Accounts > Contact Settings > Private List**.

A list of all private contact lists available in the OpenScape system is displayed in the work area.

- 4) Select the radio button of the **PrivateContactList-Service** contact list.
- 5) Click **Set Default Contact Lists**.
- 6) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 7) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 8) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 9) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

- 10) Search the list for the **VD GW Connector** component and click on the associated component name.

The dialog with the settings of the VD GW connector opens.

- 11) Specify the **false** value under **ConnectorWritableCapability**.

NOTICE: When you change the value to **false** the **PrivateGroupwareContacts-Service** will be displayed in the **Contact settings > Global List**, instead of being displayed in the **Contact settings > Private List**.

- 12) Click on **Save** to copy the settings.

- 13) Click on  in the list entry of the component **VD GW Connector** to open the action menu of the VD GW connector.

IMPORTANT: By the following step, the VD GW connector service will be stopped and immediately restarted without

any further query. This interrupts the groupware services of the OpenScape system.

-
- 14) In the actions menu, select **Restart**.

The VD GW connects is rebooted.

- 15) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 16) In the navigation tree, click **Accounts > Contact Settings > Global List**.

A list of all global contact lists available in the OpenScape system is displayed in the workspace.

- 17) Select the check box of the **PrivateGroupwareContacts-Service** contact list.

- 18) Click on **Save current selection**.

- 19) Execute the following command to reboot OpenScape UC Application, thus activating the modified settings:

```
/etc/init.d/symphoniad restart
```

OpenScape users have now only read-access to their respective private groupware contacts.

6.11.12 Handling Groupware Exchange Contact Pictures

When the Groupware Connector is activated, pictures can be added to Microsoft Exchange contacts and appear in OpenScape Web Client.

NOTICE: The contact picture file size must not exceed 15KB and the picture must be available in one of the following formats: *.jpg, *.gif, *.png.

NOTICE: If the Exchange Server is in version 2013 or greater then you should further change the value of the property exchange.server.version of the Groupware Exchange Webservices SGDO backend provider to EXCHANGE2010. The allowed value for the property exchange.server.version is: EXCHANGE2010

To enable this feature, follow the steps below:

- 1) Click on the Inventory menu item on the Maintenance navigation tab of the CMP.

- 2) In the navigation tree, click on Nodes.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click on the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click Show next to Show services status.

The services status list opens.

- 5) In the component filter, add *Groupware Exchange Webservices SGDO backend provider and click Go.

The Component page opens.

- 6) Click on the component name.
- 7) Under Properties, set the value of the property `exchange.contacts.picturesupport` to true.
- 8) Click Save.

The feature is enabled.

NOTICE: This feature is disabled by default. Every time a picture is requested, it is fetched from the Exchange server, as it is not a cached contact property. This can lead to performance or time-out issues in large contact lists or slow Exchange servers.

6.12 Managing Instant-Messaging Connections

This chapter provides information about the following topics:

- [Concept of the Instant Messaging Connection](#)
- [Displaying / Editing Instant-Messaging Connections](#)

6.12.1 Concept of the Instant Messaging Connection

You can connect the OpenScape system to an Instant Messaging server via the XMPP protocol. This enables OpenScape users to communicate with other users via Instant Messaging connections.

For the time being the OpenScape system can only provide Instant Messaging services XMPP if it is used in combination with the Openfire server. In this configuration user information is automatically synchronized between OpenScape UC Application and Openfire server.

If OpenScape UC Application is connected to an Openfire server, the IM media presence status of OpenScape users is displayed in the OpenScape clients. OpenScape UC Application determines this IM media presence status from whether or not an OpenScape user is logged in at the Openfire server and / or at the instant-messaging service. A user can explicitly log on to / log out of the instant messaging service.

6.12.2 Displaying / Editing Instant-Messaging Connections

How to display or edit the settings of the instant-messaging connection:

- 1) On the **Configuration** navigation tab of the click on the **Unified Communications** navigation menu item.

- 2) In the navigation tree, click on **Configuration > Presence & IM**.

A window opens displaying the settings of the instant-messaging connection.

You can edit the following connection settings:

NOTICE: After you have selected the **Start Openfire preconfiguration** button for an instant-messaging connection, you can only change the settings **XMPP Server IP Address** and **Admin Port**. All other settings become editable again when the connection data of a non-preconfigured Openfire server is configured for the instant-messaging connection and subsequently the **Test** button is enabled.

- **XMPP Domain Name**

Name of the XMPP domain for which the Openfire server is configured.

- **XMPP Server IP Address**

IP address of the computer system on which the Openfire server is installed.

NOTICE: When there is a solution with an integrated simplex and an integrated openfire installed, then the connection configured on CMP (under Presence / IM for openfire connection) should be the integrated openfire IP. If in this case another IP (e.g. external openfire) is configured, then UI patching will fail.

NOTICE: After you have changed the **XMPP Server IP Address** setting, always check the validity of the address used via **Test**.

- **Admin Port**

Port number via which the Openfire server can be accessed for administrative purposes. For unencrypted access via HTTP this port number is **9090**, for encrypted access via HTTPS the port number is **9091**.

- **Test**

Checks whether the Openfire server can be reached under the specified access data.

- **Openfire Database deployment**

Specifies which database OpenScape UC Application uses: the MySQL database of the Openfire server installed on an independent computer system or the SolidDB, which is an integral part of OpenScape UC Application.

Select option **MySQL** for Very Large Deployment and **Embedded DB** for all other deployment scenarios.

- **MySQL Host**

Host name of the computer system on which the MySQL database is installed. If you have selected **Embedded DB** under **Openfire Database deployment**, leave this field empty.

- **MySQL database name**

Name of the MySQL database. If you have selected **Embedded DB** under **Openfire Database deployment**, leave this field empty.

- **MySQL User**

Name of the user account privileged to access the specified database. If you have selected **Embedded DB** under **Openfire Database deployment**, leave this field empty.

- **MySQL Password (incl. repetition)**

Valid password for the specified user account. If you have selected **Embedded DB** under **Openfire Database deployment**, leave this field empty.

- **Start Openfire Admin UI**

Starts the web-based configuration interface of the Openfire server.

NOTICE: The **Start Openfire Admin UI** button does not become active until you have checked via **Test** whether the Openfire server can be reached under the specified access data. Furthermore, the Openfire server must have been pre-configured via **Start Openfire Preconfiguration**.

- **Start Openfire Preconfiguration**

Transmits a general pre-configuration to the Openfire server that prepares the instant-messaging connection to OpenScape UC Application.

NOTICE: The **Start Openfire Preconfiguration** button does not become active until you have checked via **Test** whether the Openfire server can be reached under the specified access data.

NOTICE: The general preconfiguration can be transmitted to the Openfire server only once. The transmission disables the **Start Openfire Preconfiguration** button. To transmit the preconfiguration to the Openfire server once more, set the <setup> parameter to false in the following file: /opt/openfire/conf/openfire.xml The **Start Openfire Preconfiguration** button becomes subsequently active again.

NOTICE: As a rule, the application computers of several clusters are connected to the same Openfire server in Very Large Deployment. From connecting the respectively second cluster the preconfiguration has already been transmitted to the Openfire server once. In this case you

need to transmit the preconfiguration to the respective Openfire server only for the respectively first connection. Simply specify the settings under **XMPP Server IP Address** and **Admin Port** for all further connections. Then select **Test**. After a successful connection test, back up the settings made with **Save** and close the configuration dialog.

6.13 Backing up and restoring general OpenScape System Components

IMPORTANT: With the configuration of Single Sign-On for clients, a KEYTAB file `krb5.keytab` was created. The KEYTAB file `krb5.keytab` in the `/opt/siemens` directory of a UC Application computer system is not automatically backed up when you perform a backup via the CMP. Therefore, you must back up the relevant KEYTAB file manually lest it gets lost during a system restore. After the restore you must copy the KEYTAB file in the correct directory also manually.

NOTICE: Manual *OpenScape Common Management Platform, Configuration and Administration* provides general information about backing up and restoring.

This chapter provides information about the following topics:

- [General Memory Requirements for backing up Data of the Application Computer](#)
- [Backing up a File System for a Deployment Scenario different from Integrated Deployment manually](#)
- [Restoring OpenScape Configuration Data](#)
- [Restoring the OpenScape System for Integrated Deployment](#)
- [Restoring UC Application for a Deployment Scenario different from - Integrated Deployment](#)
- [Restoring OpenScape Voice for a Deployment Scenario different from - Integrated Deployment](#)
- [Restoring the Response File from a Backup Set](#)

6.13.1 General Memory Requirements for backing up Data of the Application Computer

The following memory requirements apply for backing up the configuration and the OpenScape UC Application database.

- System configuration: approximately 200 – 300 MB
- System database: approximately 20 MB plus 200 kByte per UC Application user

The amount of memory required for backing up the file system of a UC Application computer system cannot be predicted. The memory requirements

depend in particular on the logging information collected and stored before the data backup.

6.13.2 Backing up a File System for a Deployment Scenario different from Integrated Deployment manually

IMPORTANT: To back up the file system of a UC Application computer system for a deployment scenario different from Integrated Deployment, the hard disk drives of the relevant computer system must use the file system ext3 on LVM2.

IMPORTANT: To back up a non-LVM-based file system of a UC Application computer system for a deployment scenario different from Integrated Deployment requires installing the dump RPM package on the relevant computer system.

IMPORTANT: If you back up the file system of an LVM-based UC Application computer system, the backed up data is temporarily stored in the following directory of the relevant computer system: /backups. In this case, if you use an archive that deploys the **FTP / SFTP** protocol for backing up the system, the backed up data is automatically copied to the external FTP / SFTP server and deleted in the temporary directory after completion of the backup. If, in contrast, you use an archive that deploys the **HD** protocol for backing up the system, the backed up data is always stored on the relevant computer system in the directory of the Backup Sets used. After completion of the backup process you need to copy the backed up data manually to an external computer system and delete it then from the original directory.

IMPORTANT: If you back up the file system of a non-LVM-based UC Application computer system, the backed up data is always stored on the relevant computer system in the directory of the backup set used. If in this case you back up the system using an archive that deploys the HD protocol you need to manually copy the backed up data to an external computer system and delete it in the original directory after the system backup.

IMPORTANT: Ideally, back up the archives of the OpenScape system on an external computer system. This way you avoid irretrievably losing backed up data in case of a system crash. And it saves memory on the OpenScape computer system, too.

Besides the automatic backup using backup schedules, you can also back up the file system of UC Application computer systems for a deployment scenario different from Integrated Deployment manually also.

Via the file system backup of a UC Application computer system, you can completely restore the relevant computer system after a critical system crash.

How to start the file system backup manually:

- 1) Change the sudo access settings in the sudoers file once. In doing so, always use the text editor visudo.

NOTICE: The text editor visudo checks the syntax of the sudoers file before the backup. Typing errors in the sudoers file that may hamper regular access to the computer system are thus ruled out.

- a) Open the sudoers file in the text editor visudo by executing the following command as root:

```
visudo -f /etc/sudoers
```

- b) Attach the following line to the end of the file:

```
sym ALL=NOPASSWD:/opt/siemens/servicetools/backup/fsBackup.sh
```

You must perform these changes on every UC Application computer system.

- 2) Switch to the CMP.
- 3) Select the desired domain in the **Domain** drop-down list of the toolbar.
- 4) On the **Maintenance** navigation tab click on the **Recovery** navigation menu item.
- 5) In the navigation tree, click on Backup & Restore > Backup.
The backup wizard dialog opens.
- 6) Select the archive in which the file system backup is to be stored:
 - If you wish to back up the file system via the **FTP** or **SFTP** protocol, either select an existing archive with the ... button or create a new archive with the **Add** button.
 - If you wish to back up the file system via the **HD** protocol, select the **DEFAULT** archive in the **Select archive** field with the ... button.
- 7) If required, enter a comment for your backup set in the **Comment** field.
- 8) Click on **Next**.
- 9) In the **Select backup type** drop-down list, select the **System** option.
- 10) Click on the backup unit **Application Server** and select the check box for the following option:
 - **FileSystem Backup**
- 11) Click on **Save**.
- 12) Click on **Start**.

The backup of the file system starts. In this process, the file systems for all UC Application computer systems of a deployment scenario different from Integrated Deployment are backed up. While the backup job is being carried out, a percentage display informs you continuously about the current backup progress.

The backup progress is graphically shown in the **Last job status** dialog.

- 13) If you wish to back up the file system of a non-LVM-based UC Application computer system using an archive that deploys the HD protocol, you need

to manually copy the backed up data to an external computer system and delete it in the original directory.

You find the backed up data in the directory of the backup set used. It is contained in a TAR file the name of which has the following format:

`<node name>_Bkup__<month>_<day>_<year>_<time>.tar`

Example of created backup files from a very large deployment:

- BackupSetInfo.xml
- BackupUnit_FileSystemBackup_Info.xml
- Package_FileSystemBackup_FileSystemBackup_001.xml
- Package_FileSystemBackup_FileSystemBackup_001.zip
- Package_FileSystemBackup_FileSystemBackup_002.xml
- Package_FileSystemBackup_FileSystemBackup_002.zip
- Package_FileSystemBackup_FileSystemBackup_003.xml
- Package_FileSystemBackup_FileSystemBackup_003.zip
- ucsymVBE__boot.backup.tar.gz
- ucsymVBE__mbr_sda
- ucsymVBE__OpenscapeUC1.vg_backup
- ucsymVBE__OpenscapeUC2.vg_backup
- ucsymVBE__OpenscapeUCRoot.vg_backup
- ucsymVBE__opt_siemens.backup.tar.gz
- ucsymVBE__partition.info
- ucsymVBE__pv_backup
- ucsymVBE__root.backup.tar.gz
- ucsymVBE__var_siemens.backup.tar.gz
- ucsymVFE__boot.backup.tar.gz
- ucsymVFE__mbr_sda
- ucsymVFE__OpenscapeUC1.vg_backup
- ucsymVFE__OpenscapeUC2.vg_backup
- ucsymVFE__OpenscapeUCRoot.vg_backup
- ucsymVFE__opt_siemens.backup.tar.gz
- ucsymVFE__partition.info
- ucsymVFE__pv_backup
- ucsymVFE__root.backup.tar.gz
- ucsymVFE__var_siemens.backup.tar.gz
- ucsymVMS__boot.backup.tar.gz
- ucsymVMS__mbr_sda
- ucsymVMS__OpenscapeUC1.vg_backup
- ucsymVMS__OpenscapeUC2.vg_backup
- ucsymVMS__OpenscapeUCRoot.vg_backup
- ucsymVMS__opt_siemens.backup.tar.gz
- ucsymVMS__partition.info
- ucsymVMS__pv_backup
- ucsymVMS__root.backup.tar.gz
- ucsymVMS__var_siemens.backup.tar.gz

IMPORTANT: When you back up the file systems for a deployment scenario different from Integrated Deployment, you may have to shift the backed up data from each UC Application computer system to an external computer system. You find related information in the notes at the beginning of this section. The backed up data must be shifted to a harddisk formatted with ext2 or ext3. The free

memory on the harddisk used must be four times larger than the backed up data.

- 14) How to back up the file system of an LVM-based UC Application computer system:

- a) Copy the backed up data manually to an external computer system and delete it then from the original directory.

You find the backed up data in the following directory of the relevant computer system: /backups

NOTICE: When you back up the file systems for a deployment scenario different from Integrated Deployment, you may have to shift the backed up data from each UC Application computer system to an external computer system. You find related information in the notes at the beginning of this section. The backed up data must be shifted to a harddisk formatted with ext2 or ext3. The free memory on the harddisk used must be four times larger than the backed up data.

- b) Copy the restore script `Restore.sh` to the same location on the external computer system to which you shifted the backed up data.

You find the restore script in the following directory of the UC Application computer system:

`<Osc-Install23>/servicetools/backup`

- 15) If Single Sign-On has been configured for clients:

Back up the KEYTAB file `krb5.keytab` manually.

You find this file in the following directory:

- For Small Deployment:

In the `/opt/siemens` directory of the application computer (active and, if required, passive)

- For all other deployment scenarios:

In the `/opt/siemens` directory of the front-end computers

6.13.3 Restoring OpenScape Configuration Data

By using a backup set, you can partly or completely restore the configuration data of the OpenScape system. This requires the following:

- You have previously saved the information to be restored in an archive.
- The archive's data are not damaged.

NOTICE: When using a backup set you have temporarily backed up on another computer system please heed the following: Copying the backup file assigns it to user **root** and group **root**. It must however be reassigned to user **sym** and

²³ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

group **sym** for restoring the configuration data. This can be done via the following command: `chown sym:sym <file name>`

How to restore the configuration data of the OpenScape system:

- 1) Check whether the following conditions apply:
 - You wish to restore the configuration data for a deployment scenario different from Integrated Deployment.
 - You have just restored the application computer by a new installation with the original response file.
 - You have expanded the original deployment scenario retrospectively by at least one front-end or Media Server computer.

If **all** of these conditions apply, follow the instructions given in this step. If one of these conditions does not apply, continue with step 2.

 - a) Open the following file in a text editor on the application computer.
`/opt/siemens/common/conf/system.xml`
 - b) Open the following file on the retrospectively installed Media Server or front-end computer in a text editor.
`/opt/siemens/common/conf/system.xml`
 - c) In the `system.xml` file of the Media Server computer or front-end computer look for the configuration section `<NodeList>`.
 - d) Look for the entry of the newly installed Media Server computer or front-end computer in the configuration section `<NodeList>`.
 - e) Copy the relevant entry to the corresponding location in the `system.xml` file of the application computer.
 - f) Execute steps b to e for every newly installed Media Server computer and front-end computer.
 - g) Save the supplemented `system.xml` file of the application computer under its existing name.
 - h) If you have not yet stopped the application computer and all Media Server computers and front-end computers of the OpenScape system, do it now with the following command.
`/etc/init.d/symphoniad stop`
 - i) Start the application computer with the following command:
`/etc/init.d/symphoniad start`
 - j) After the application computer has started, wait for a minute and start all Media Server computers and front-end computers of the OpenScape system with the following command.
`/etc/init.d/symphoniad start`
- 2) Execute one of the following commands as root on the application computer to stop the web server component:
 - **For deployment scenarios without front-end computer:**
`/etc/init.d/symphoniad stop WebClient`
 - **For deployment scenarios with front-end computer:**
`/etc/init.d/symphoniad stop WebClient_BE`
- 3) Invoke the CMP and log on under the ID **administrator@system**.

- 4) Select in the **Domain** drop-down list of the CMP toolbar the domain the configuration data of which you wish to copy.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 5) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.

- 6) In the navigation tree, click on Backup & Restore > Restore.

The restore wizard dialog opens.

- 7) Use the ... button in the **Select archive** field to select the archive in which the backup set with the desired configuration data has been stored.

- 8) Click on **Next**.

- 9) Select the backup set for restoring the configuration data.

- 10) Click on **Next**.

The backup units of the selected backup set are displayed.

- 11) Select the backup units you wish to restore.

- 12) Click on **Start restore**.

The restore starts according to the settings made. The restore progress is then displayed graphically.

- 13) After completion of the restore procedure execute one of the following commands on the application computer of OpenScape UC Application as root to restart the previously stopped web server component:

- **For deployment scenarios without front-end computer:**

```
/etc/init.d/symphoniad start WebClient
```

- **For deployment scenarios with front-end computer:**

```
/etc/init.d/symphoniad start WebClient_BE
```

Restoring the configuration data is now complete.

6.13.4 Restoring the OpenScape System for Integrated Deployment

You can restore the OpenScape system for Integrated Deployment after a critical system crash. To do this, you must reinstall the OpenScape software on the OpenScape computer system and subsequently import the configuration data into the newly installed system.

This requires the following:

- The hardware of the computer system to be restored has not been damaged.
- You backed up the configuration data of the OpenScape system in an archive before the crash.
- The backed up data has not been damaged by the crash.

After being restored, the OpenScape system is fully functional again and works with the configuration data existing when the configuration data backup was performed.

How to restore the OpenScape system for Integrated Deployment after a system crash:

- 1) Reinstall the OpenScape software on the OpenScape computer system.

When reinstalling, definitely use the response file you have created for the initial installation. This is because:

- The Symphonia community name must be the same for the initial and reinstallation.
- The administrator password for the system database must be the same for the initial and reinstallation. The import feature is otherwise unable to restore the database.
- The IP addresses and host names must be the same for the initial and reinstallation, since they are referenced in the data that will later restore them.

NOTICE: If you have not manually backed up the response file after the initial installation, you can restore it from the information of a system backup independent from the other backup data. This requires you having saved the file with a backup. How to restore the response file from the information of a system backup is described in [Restoring the Response File from a Backup Set](#) on page 460.

NOTICE: If you restore the system on another computer system, disconnect the original computer system from the network. When you reconnect the original computer system to the network under a different IP address, verify that all OpenScape components are inactive on this computer system.

- 2) Before starting OpenScape UC Application, delete the contents of these two log files.

- /log/osgi.log
- /log/osgi.err

These files include the system start log information.

- 3) Execute the following command on the computer system on which you have installed OpenScape UC Application.

```
/etc/init.d/symphoniad start
```

OpenScape UC Application starts. While the system starts, the system start log should not log any errors.

After the following message in the system start-up log, all OpenScape UC Application services are up and running.

```
***** Starting all instances done. *****
```

Depending on the system configuration, it may take several minutes until all users configured in the system have been activated.

- 4) Execute the following command to put out the system startup log.

```
tailf /log/osgi.log
```

- 5) Open the following error log file after the OpenScape UC Application startup has finished.

```
/log/osgi.err
```

The error log file should not contain an error message.

- 6) Execute the following command as root to stop the web server component.

```
/etc/init.d/symphoniad stop WebClient
```
- 7) On the reinstalled OpenScape computer system, access the CMP and log on with the following ID: **administrator@system**.
- 8) Select in the **Domain** drop-down list of the CMP toolbar the domain the configuration data of which you wish to copy.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 9) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 10) In the navigation tree, click on Backup & Restore > Restore.
The restore wizard dialog opens.
- 11) Use the ... button in the **Select archive** field to select the archive in which the backup set with the desired configuration data has been stored.
- 12) Click on **Next**.
- 13) Select the backup set for restoring the configuration data.

NOTICE: When using a backup set you have temporarily backed up on another computer system please heed the following: Copying the backup file assigns it to user **root** and group **root**. It must however be reassigned to user **sym** and group **sym** for restoring the configuration data. This can be done via the following command: `chown sym:sym <file name>`

- 14) Click on **Next**.
The backup units of the selected backup set are displayed.
- 15) Select the backup units you wish to restore.
- 16) Click on **Start restore**.
The restore starts according to the settings made. The restore progress is then displayed graphically.
- 17) Reboot OpenScape UC Application with the following commands:

```
/etc/init.d/symphoniad stop  
/etc/init.d/symphoniad start
```
- 18) The password for the **administrator@system** administrator account is after the data restoration reset to the value that was valid when the configuration files were backed up. If you want to reset the password of

the **administrator@system** administrator account, execute the following command.

```
<Osc-Install24>/servicetools/security/resetUserAccount.sh  
administrator@system '<new password >'
```

NOTICE: Enclose the new password in single quotation marks to prevent the operating system from misinterpreting the entry. *Example:* /enterprise/servicetools/security/resetUserAccount.sh administrator@system 'd7Rej!1eD'

19) If Single Sign-On was configured for clients:

Copy the manually backed up KEYTAB file `krb5.keytab` to the following directory of the application computer (active and, if required, passive computer).

```
/enterprise
```

You have now restored the OpenScape computer system for Integrated Deployment after a critical system crash.

6.13.5 Restoring UC Application for a Deployment Scenario different from Integrated Deployment

NOTICE: If you restore the system on another computer system, disconnect the original computer system from the network. When you reconnect the original computer system to the network under a different IP address, verify that all OpenScape components are inactive on this computer system.

You can restore every UC Application computer system of a deployment scenario different from Integrated Deployment after a critical system crash by restoring the file system of the relevant computer system.

This requires the following:

- The hardware of the UC Application computer system to be restored has not been damaged.
- You backed up the file system of the relevant UC Application computer system before the crash.
- The backed up data is stored on an external computer system.

NOTICE: The backed up data must have been stored on a harddisk formatted with ext2 or ext3. The free memory on the harddisk used must be three times larger than the backed up data.

- The backed up data has not been damaged by the crash.
- If you wish to restore the file system of an LVM-based UC Application computer system: You have copied the restore script `Restore.sh` to the

²⁴ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

same location on the external computer system like the backed up data of the UC Application computer system. Compare [Backing up a File System for a Deployment Scenario different from Integrated Deployment manually](#) on page 449.

After the restoration of the file system, the relevant UC Application computer system is fully functional again and works with the configuration data existing when the file system backup was performed.

How to restore a UC Application computer system for a deployment scenario different from Integrated Deployment after a system crash:

- 1) Insert the installation data carrier of the Linux operating system into the disk drive of the computer system you want to restore.
- 2) Reboot the computer system.
The computer system boots in the rescue mode.
- 3) Mount the data carrier on which the backup file of the file system is stored.
- 4) On the data carrier access the directory in which the backup file of the file system is stored.
- 5) How to restore the file system of a non-LVM-based UC Application computer system:

- a) Execute the following command to unzip the non-LVM-based restore script with its directory from the backup file:

```
tar -xvf <backup file name> *Restore.sh
```

- b) Execute the following command to copy the unpacked non-LVM-based restore script to the current directory:

```
cp <Osc-Install25>/servicetools/backup/Restore.sh .
```

- c) Execute the following command to start the non-LVM-based restore script:

```
./Restore.sh
```

The available archives are offered to you for selection.

- d) Select the archive you wish to use for restoring.
- e) Confirm your selection.

The restore process starts and information about the single Linux-based restore commands are put out via the shell.

If an error occurs while a Linux command is being executed, you can see this in the shell. Correct the error then as is described in the Linux product documentation.

- 6) How to restore the file system of an LVM-based UC Application computer system:
 - a) Create a temporary working directory on an external USB storage medium of the UC Application computer system to be restored.

NOTICE: You need to unpack the archive of the backup files on an external storage medium. This storage

²⁵ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

medium must have been mounted as /mnt (mount /dev/shxxx /mnt).

- b) Unpack in this directory the archive of the backup files you want to use for restoring the UC Application computer system. To do this, use the tar command.
- c) Check that the restore script Restore.sh is found in the following directory of the unpacked backup files:

<temporary working directory>/backups

If it is missing there, copy it manually.

NOTICE: Be sure to have copied the restore script to the same place as the backed up data of the UC Application computer system during the previous data backup.

- d) Execute the following command to start the LVM-based restore script:

```
sh Restore.sh
```

The restore process starts and information about the single Linux-based restore commands are put out via the shell.

If an error occurs while a Linux command is being executed, you can see this in the shell. Correct the error then as is described in the Linux product documentation.

- 7) Wait until the restore script used announces the end of the restoration.
- 8) Take the setup data carrier of the Linux operating system out of the computer system drive.
- 9) Execute the following command on the computer system on which you have installed OpenScape UC Application.

```
/etc/init.d/symphoniad start
```

OpenScape UC Application starts. While the system starts, the system start log should not log any errors.

After the following message in the system start-up log, all OpenScape UC Application services are up and running.

```
***** Starting all instances done. *****
```

Depending on the system configuration, it may take several minutes until all users configured in the system have been activated.

- 10) Execute the following command to put out the system startup log.

```
tailf /var/siemens/common/log/osgi.log
```

- 11) Open the following error log file after the OpenScape UC Application startup has finished.

```
/var/siemens/common/log/osgi.err
```

The error log file should not contain an error message.

- 12) The password for the **administrator@system** administrator account is after the data restoration reset to the value that was valid when the configuration files were backed up. If you want to reset the password of

the **administrator@system** administrator account, execute the following command.

```
<Osc-Install26>/servicetools/security/resetUserAccount.sh  
administrator@system '<new password >'
```

NOTICE: Enclose the new password in single quotation marks to prevent the operating system from misinterpreting the entry. *Example:* /enterprise/servicetools/security/resetUserAccount.sh administrator@system 'd7Rej!1eD'

13) If Single Sign-On was configured for clients:

Copy the manually backed up KEYTAB file krb5.keytab to the following directory:

- For Small Deployment:
To the /opt/siemens directory of the application computer (active and, if required, passive)
- For all other deployment scenarios:
To the /opt/siemens directory of the front-end computers

You have now restored the UC Application computer system for a deployment scenario different from Integrated Deployment after a critical system crash.

6.13.6 Restoring OpenScape Voice for a Deployment Scenario different from Integrated Deployment

How to restore the independent OpenScape Voice system for a deployment scenario different from Integrated Deployment describes the product documentation of OpenScape Voice.

6.13.7 Restoring the Response File from a Backup Set

You can restore the OpenScape system after a critical system crash. For this purpose you definitely need to use the response file that you have created for the initial setup.

If you have not manually backed up the response file after the initial installation, you can restore it from the information of a system backup independent from the other backup data. This requires you having saved the file with a backup.

The response file is stored in one of the following zip files in the relevant backup set by default.

- For an unencrypted backup set in:
Package_Install_installbase_001.zip

²⁶ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

- For an encrypted backup set in:

Package_Install_installbase_001.z

NOTICE: In deployment scenarios with several computer systems there is an individual zip file for each computer system. In the following section of the response file you can see for which computer system a response file applies:

Example of an application computer:

```
# Local host Settings
SI_LOCAL_HOST=10.25.100.211
SI_LOCAL_NAME=Backend_Server
SI_LOCAL_TYPE=BACKEND
```

How to restore the response file from the information of a system backup:

- 1) Place the OpenScape product data carrier in the drive of the computer system on which you want to reinstall OpenScape UC Application.
- 2) If the backup set with the enclosed response file was created encrypted, execute the following steps:
 - a) Switch to the following directory on the product data carrier:

/configurator

- b) Execute the following command to decode the encrypted passwords in the response file:

```
./run.sh decrypt <zip file> -p <password> -o <output file>
```

Meaning of the wildcards:

<zip file> - Name of the zip file in which the response file is backed up and the path to the file.

<password> - Password used for encrypting the backup set.

<output file> - Zip file in which the response file is stored packed up after the decryption.

Example:

```
./run.sh decrypt /var/siemens/backup/
london/BackupSet_090713_110201/
Package_Install_installbase_001.z
-p test -o /tmp/decrypt.zip
```

NOTICE: The run script is shipped on the product data carrier of OpenScape UC Application and is also used for the OpenScape system setup.

- 3) Open the zip file that contains the response file.
 - For an unencrypted backup set this is the following file in the backup set by default:
Package_Install_installbase_001.zip
 - For an encrypted backup set this file is the decoded output file from step [2](#).
- 4) Unpack the response file from the relevant zip file.

- 5) Switch to the following directory on the product data carrier:
/configurator
- 6) Execute the following command to start the setup configurator of OpenScape UC Application.
./run.sh
- 7) Select the **Use existing response file** option and use the response file you have restored from the backup archive.
- 8) Execute the setup configurator without changing the response file settings.

NOTICE: The fields for the administrator password do not show any information, since the encrypted password of the response file is not displayed in the configurator.

You can use the concludingly backed up response file to reinstall an OpenScape system.

6.14 Managing the Voice Portal

This chapter provides information about the following topics:

- [Creating an individual User Access](#)
- [Creating an individual Guest Access](#)
- [Configuring the Default Language of a Voice Portal Access](#)
- [Changing the Phone Number Use by the Voice Portal in Case of Forwardings](#)

6.14.1 Creating an individual User Access

You can add user accesses with individual settings to the voice portal applications. Such a new user access is based on an individual voice portal application profile, which is assigned to a new Media Server terminal.

Start the configuration

How to create a new user access with individual settings for a voice portal application:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select in the list the link of the voice portal application for which you wish to configure a user access.
 - Select the **Voiceportal** application, if you wish to configure a user access controlled via telephone keys.
 - Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled user access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 6) Select the radio button of the application profile **start (Voice Portal access)** and select **Copy**.

The configuration dialog for a new application profile opens.

- 7) Specify under **Profile name** a name for the new application profile.

The application profile will be managed in the voice portal plug-in under this name.

- 8) Check that the **General** tab is displayed.
- 9) Select under **Voice Portal default language** the default language for the user access to deploy.
- 10) If required, perform further individual user access settings.
- 11) Click on **Save** to copy the settings for the application profile.
- 12) Click on **Close** to close the configuration dialog of the voice portal plug-in.
- 13) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
- 14) Select **Add**.

The configuration dialog for a new terminal opens.

- 15) Specify a unique identifier for the new terminal under **Terminal ID**.

The terminal is administered in the CMP under this identifier.

- 16) Select the voice portal application profile you have just created under **Application**.
- 17) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

- 18) Specify under **Address-expression** at least one phone number under which the guest access shall be available.

NOTICE: Calls for the defined phone numbers must be routed to the SIP trunk to the OpenScape Media Server by the communications system used. You need to configure the routing of the communications system accordingly.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

- 19) Determine under **Type** in which format the specified address expression is to be interpreted by the OpenScape Media Server.
- 20) Click on **OK** to copy the address settings.
- 21) If required, bind further addresses to the terminal in the described manner.
- 22) Click on **Save** to copy the settings for the terminal.

- 23) If required, configure in the described manner further voice portal user accesses – e. g. user accesses with other default languages.

You have now created a new user access with individual settings for a voice portal application.

6.14.2 Creating an individual Guest Access

You can add guest accesses with individual settings to the voice portal applications. Such a new guest access is based on an individual voice portal application profile, which is assigned to a new Media Server terminal.

Start the configuration

How to create a new guest access with individual settings for a voice portal application:

- 1) In the configuration dialog of the selected OpenScape Media Server switch to the **Applications** tab.
You see a list of all applications that are active in the selected OpenScape Media Server.
- 2) Select in the list the link of the voice portal application for which you wish to configure a guest access.
 - Select the **Voiceportal** application, if you wish to configure a telephone-controlled guest access.
 - Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled guest access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 3) Select the radio button of the application profile **guest (Guest Portal access)** and select **Copy**.

The configuration dialog for a new application profile opens.

- 4) Specify under **Profile name** a name for the new application profile.

The application profile will be managed in the voice portal plug-in under this name.

- 5) Check that the **General** tab is displayed.
- 6) Select under **Voice Portal default language** the default language for the guest access to deploy.
- 7) If required, perform further individual user access settings.
- 8) Click on **Save** to copy the settings for the application profile.
- 9) Click on **Close** to close the configuration dialog of the voice portal plug-in.
- 10) In the OpenScape Media Server configuration dialog switch to the **Terminals** tab.
- 11) Select **Add**.

The configuration dialog for a new terminal opens.

- 12) Specify a unique identifier for the new terminal under **Terminal ID**.

The terminal is administered in the CMP under this identifier.

- 13) Select the voice portal application profile you have just created under **Application**.

- 14) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

- 15) Specify under **Address-expression** at least one phone number under which the guest access shall be available.

NOTICE: Calls for the defined phone numbers must be routed to the SIP trunk to the OpenScape Media Server by the communications system used. You need to configure the routing of the communications system accordingly.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

- 16) Determine under **Type** in which format the specified address expression is to be interpreted by the OpenScape Media Server.
- 17) Click on **OK** to copy the address settings.
- 18) If required, bind further addresses to the terminal in the described manner.
- 19) Click on **Save** to copy the settings for the terminal.
- 20) If required, configure in the described manner further voice portal guest accesses – e. g. guest accesses with other default languages.

You have now created a new guest access with individual settings for a voice portal application.

6.14.3 Configuring the Default Language of a Voice Portal Access

The voice portal plays the first announcements always in a language which is independent of the calling user. This is the so-called default language which can be defined individually for the terminal of each voice portal access.

Only after the calling user has logged in to the voice portal, the portal tries to determine the user-individual language setting. To do this, it searches in the OpenScape user database for the individual user settings based on the logon data used. If the determined user-individual language setting is different from the default setting, the voice portal switches the TUI to the language determined. This requires that the language determined is available for the voice portal.

NOTICE: If a user reaches the voice portal via an XPR Server (Trusted Transfer Mode), the voice portal does not determine the user-individual language setting via the OpenScape user database. The user-individual language setting is transferred to the voice portal by the XPR Server instead.

If the language determined is not available for the voice portal, the TUI will still be played in the default language. To guests, the voice portal announcements can only be played in the default language.

If you wish to offer a user interface of the voice portal in several default languages, you need to configure an individual voice portal application profile for each desired language and assign it to an individual terminal.

If no individual default language is defined for a voice portal access, English (United States) is pre-set as default language.

Start the configuration

How to configure the default language for an individual voice portal application profile:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.
You see a list of all Media Servers available in the OpenScape system.
- 3) In the list select the OpenScape Media Server link that you want to configure.
The configuration dialog of the selected OpenScape Media Server opens.
- 4) In the configuration dialog switch to the **Applications** tab.
You see a list of all applications that are active in the selected OpenScape Media Server.
- 5) Select in the list the link of the voice portal application for which you wish to configure the voice portal access.
 - Select the **Voiceportal** application, if you wish to configure a voice portal access controlled via telephone keys.
 - Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled voice portal access.The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.
- 6) Enable the radio button of the application profile for which you wish to configure the default language.
- 7) Select **Edit**.
The configuration dialog for the application profile opens.
- 8) Check that the **General** tab is displayed.
- 9) Select under **Voice Portal default language** the default language for the application profile to deploy.
- 10) Click on **Save** to copy the settings for the application profile.
- 11) Click on **Close** to close the configuration dialog of the voice portal plug-in.

You have now configured the default language for the selected application profile. All voice portal accesses the terminal of which has been assigned the relevant application profile now use this default language.

6.14.4 Changing the Phone Number Use by the Voice Portal in Case of Forwardings

If the voice portal receives a repeatedly forwarded call, it uses the phone number from which the call was forwarded initially as originator number by default.

Alternatively, the voice portal guest accesses can use the phone number as originator number from which the call was forwarded last.

Start the configuration

Execute the following configuration steps to make a guest access use the phone number as originator number from which the call was forwarded last.

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select in the list the link of the voice portal application for which you wish to configure the voice portal access.
 - Select the **Voiceportal** application, if you wish to configure a voice portal access controlled via telephone keys.
 - Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled voice portal access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

- 6) Enable the radio button of the guest access application profile for which you wish to configure the phone number use.
- 7) Select **Edit**.

The configuration dialog for the application profile opens.

- 8) Check that the **General** tab is displayed.
- 9) Deactivate the option **First redirected number of the list**.
- 10) Click on **Save** to copy the settings for the application profile.
- 11) Click on **Close** to close the configuration dialog of the voice portal plug-in.

You have now configured the phone number use for the selected application profile. All voice portal accesses the terminal of which has been assigned the relevant application profile now deploy this type of phone number use.

6.15 Managing the Conference Portal

This chapter provides information about the following topics:

- [Configuring Security Settings for outgoing Conference Connections](#)
- [Configuring the Default Language for outgoing Conference Connections](#)
- [Configuring the Conference Portal Access for another existing Language](#)
- [Changing Music-on-Hold for the Conference Portal](#)
- [Restricting Media Types and Locations for Conference Services](#)
- [Configuring the maximum Number of Conference Participants](#)

- [Changing the E-Mail Notification Text for Conferences](#)
- [Changing the Participant Signaling Restriction](#)
- [Disabling the Full HD Resolution](#)
- [Configuring Video Layouts used](#)
- [Configuring Mailbox Recognition of the Conference Portal](#)
- [Managing Video Layouts for Conferences](#)
- [Managing Conferences independently of OpenScape UC Application](#)

6.15.1 Configuring Security Settings for outgoing Conference Connections

You can define with which security settings the OpenScape Media Server establishes outgoing conference connections.

NOTICE: You define the security settings for incoming conference connections in the address binding for the corresponding conference portal access.

Start the configuration

How to configure the security settings for outgoing conference connections:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Media Server**.
You see a list of all Media Servers available in the OpenScape system.
- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Terminals** tab.
- 5) In the terminals list, select the terminal with the terminal ID **conferencing-callout**.

The configuration dialog of the relevant terminal opens.

NOTICE: The conference portal uses the **conferencing-callout** terminal only to define the settings of outgoing connections. It is not necessary to bind this terminal to a phone number.

- 6) Select the desired value under **Security mode**.
- 7) Select **Save** to copy the modified setting.

You have now configured the security settings for outgoing conference connections.

6.15.2 Configuring the Default Language for outgoing Conference Connections

When the conference portal calls a participant to join a conference, it attempts to identify this callee as OpenScape user. For this purpose, it searches the OpenScape user database for a user to whom the phone number used has been assigned as a number resource in the CMP.

If the conference portal can identify a unique user in this way, it determines the user-individual language setting by using the user settings and switches the TUI to this language, if required. This requires that the language determined is available for the conference portal.

If the determined language is unavailable to the conference portal or the callee cannot be identified via his/her originator number, the TUI language is determined by the general default language of the conference portal.

Start the configuration

How to configure the default language of the conference portal for outgoing conference connections:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) In the conferences dialog, switch to the **Configuration** tab.
- 4) Select Default language under **Media configuration**.
- 5) Under Default language, select the language that the conference portal is to use for outgoing conference connections, if it cannot identify the called participant as OpenScape user.
- 6) Select **Save** to copy the modified setting.

You have now configured the default language for outgoing conference connections.

6.15.3 Configuring the Conference Portal Access for another existing Language

After a caller has logged in to the conference portal, the conference portal tries to identify the caller as an OpenScape user. To do this, it searches the OpenScape user database for a user to whom the originator number used has been assigned as a number resource in CMP.

If the conference portal can identify a unique user in this way, it determines the user-individual language setting by using the user settings and switches the TUI to this language, if required. This requires that the language determined is available for the conference portal.

If the determined language is unavailable to the conference portal or the caller cannot be identified via his/her originator number, the TUI language must be determined in another way. In this case the TUI language is determined by the configured default language of the conference portal access via which the user is connected to the conference portal.

You can set the default language for the default access of the conference portal in the CMP's conference portal plug-in (cf. [Configuring the Default Language for outgoing Conference Connections](#) on page 469). If you wish to provide accesses with further default languages for the conference portal, you need to configure an additional conference portal access for each desired default language.

Start the configuration

How to configure an additional conference portal access for another default language:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) In the conferences dialog, switch to the **Configuration** tab.

- 4) Under Number Configuration, select **Bridge numbers**.

The Bridge numbers tab is displayed.

- 5) Select **Language dependent bridge numbers**.

The dialog for configuring language dependent bridge numbers opens.

- 6) Specify under **New number** the phone number for reaching the new conference portal access.

NOTICE: Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

- 7) Select the language the new conference portal access shall use as default language from the associated combo box.

- 8) Select **Update**.

The new bridge number is updated.

- 9) Select **Save** to create the newly updated conference portal access on the OpenScape Media Server.

If you use several OpenScape Media Servers in a Media Server farm the newly added conference portal access is added on all OpenScape Media Servers of the Media Server farm.

You have now configured another conference portal access for an additional default language.

6.15.4 Changing Music-on-Hold for the Conference Portal

IMPORTANT: The OpenScape Media Server conference portal is installed by default with music-on-hold for which no license fees need to be paid. If you change this music-on-hold, you may have to pay license fees (for example GEMA fees) for the newly configured recording. Check on this **before** you replace the music on hold.

NOTICE: The OpenScape Media Server supports only selected recording formats for music-on-hold. You can look up such formats in the *OpenScape Media Server, Administrator Documentation*.

The OpenScape Media Server conference portal provides music-on-hold. You can customize this music-on-hold for each system language of the conference portal.

Start the configuration

How to change the music-on-hold for the conference portal:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) Check that the **Providers** tab is displayed.

- 5) Select **Announcements and Resources** from the list of names.

The configuration dialog for the **Announcements and Resources** provider opens.

- 6) Check that the **Prompt and Music Files** tab is displayed.

- 7) Search the directory structure for the following entries:

Conferencing / <version> / <language> / CallControll.LoopMusic

- 8) Click on the entry's name.

The configuration dialog for the selected file opens.

- 9) Check that the **Deploy Customized Prompt** tab is displayed.

- 10) Select under **Import File** the file the recording of which is to be used instead of the default music-on-hold.

- 11) Select **Deploy now** for loading the specified file.

- 12) Select **Close**.

- 13) Change the music-on-hold in this way for all available languages as far as possible.

- 14) Select **Save** to copy the modified setting.

You have thus replaced the music-on-hold recording of the conference portal.

6.15.5 Restricting Media Types and Locations for Conference Services

The conferencing infrastructure of OpenScape UC Application is provided by the configured OpenScape Media Server. If OpenScape UC Application is operated with several OpenScape Media Servers, you can optimize audio and video conferences in particular on the basis of the following criteria and divide them between the available OpenScape Media Servers.

- Type of conference medium (audio or video)
- Geographic assignment

You can perform this setting individually for each OpenScape Media Server.

Start the configuration

How to configure the media and location an OpenScape Media Server shall provide conferences for:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) In the conferences dialog, switch to the **Configuration** tab.
- 4) Select **Bridge numbers** under Number configuration.
- 5) Switch to the Trunk numbers tab.
- 6) Select in the list of Media Server nodes the OpenScape Media Server name you wish to configure.

The configuration dialog for the selected OpenScape Media Server opens.

- 7) Switch to the **Media Server selection** tab.
- 8) Select under **Media Support** the check boxes of the media for which the OpenScape Media Server is to provide conferences, i.e. Audio only or Video.
- 9) If you want the OpenScape Media Server to provide conferences for selected locations only, execute the following steps.
 - a) Select under **Office Code** the office code of the location for which the OpenScape Media Server is to provide conferences.
 - b) Select **Add**.

The selected office code is added to the phone number list.

- c) If the OpenScape Media Server is to provide conferences for further office codes, add the office codes in the same manner.
- 10) Select **Save** to apply the changed settings for the OpenScape Media Server.
- 11) Click on **Save** to apply the changed settings for the conference portal.

You have now specified the media and location for which the relevant OpenScape Media Server provides conferences.

6.15.6 Configuring the maximum Number of Conference Participants

The conference portal allows any number of participants for each conference by default. Alternatively, you can define a maximum number of conference participants.

You can perform this setting individually for each OpenScape Media Server.

Start the configuration

How to configure the maximum number of participants per conference for an OpenScape Media Server:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) Switch to the Configuration tab.

- 4) Under Number Configuration, select **Bridge numbers**.

The Bridge numbers tab is displayed.

- 5) Select from the list of Media Server nodes the name of the OpenScape Media Server for which you want to configure the maximum number of conference participants.

The configuration dialog for the selected OpenScape Media Server opens.

- 6) Specify under **Max. number of participants** the maximum number of participants to be admitted per conference by the conference portal.

NOTICE: The entire number of conference participants is additionally limited by the performance of the OpenScape Media Server computer system. You find details about this in the *OpenScape UC Application, Planning Guide*.

- 7) Select **OK**.

- 8) Select **Save** to copy the modified setting.

You have thus determined the maximum number of participants per conference for the relevant OpenScape Media Server.

6.15.7 Changing the E-Mail Notification Text for Conferences

NOTICE: The following configuration concerns the notification text for conferences that a user configures in the OpenScape Web Client, in OpenScape Conference Extension for Microsoft - Outlook or in OpenScape Conference Extension for Lotus - Notes.

The conference portal sends e-mail notifications to conference participants on fixed occasions. The texts of such notifications are pre-configured for all conference portal TUI languages and thus available after the conference portal has been installed.

Before the conference portal sends the e-mail notification to a conference participant, it attempts to identify the participant as OpenScape user. In this process it searches the OpenScape user database for the relevant conference participant.

If the conference portal manages to identify the conference participant in this way, it determines the user-individual language setting from the user settings and sends the e-mail notification in this language then. This requires the text of the e-mail notification being available in the language thus determined.

If the text of the e-mail notification is unavailable in the determined language or the conference participant cannot be found in the OpenScape user database, the system sends the e-mail notification in English (US).

Start the configuration

How to change the text of the e-mail notification for an individual language:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

- 2) In the navigation tree, click on **Configuration > Conferences**.
The configuration dialog of the conference portal plugin opens.
- 3) Switch to the Configuration tab.
- 4) Under Other, select Notification.
The dialog for configuring e-mail notification opens.
- 5) Verify that the **Send e-mail** option is enabled. Only then, the conference portal sends e-mail notifications to conference participants.
- 6) Click in the list entry of the desired notification language on  to open the associated action menu.
- 7) In the actions menu, select **Edit**.
The dialog for changing the notification text for the selected language opens.
- 8) Verify that the desired language is displayed under **E-mail notification for language**.
- 9) The structure of the e-mail notification depends on the occasion on which it is sent. Therefore, select under **Trigger name** the occasion for which you wish to change the notification text.
Under **Included body parts** you see the names of all message parts contained in an e-mail notification for the selected occasion.
- 10) Click on **Show preview**.
You see the entire notification text for the selected occasion. The single body parts of the notification text appear in the sequence in which they are listed under **Included body parts**.
- 11) Consider which body parts of the notification text you wish to change.

NOTICE: When you change the content of an individual body part for the selected occasion, you change this body part for all other occasions that use this body part also.

- 12) Select **back to Editor**.
- 13) Specify under **Subject** a text to be used by the e-mail notification for the selected occasion.
- 14) Select under **Included body parts** the message part you wish to change.
The text of the relevant body part is displayed in the text field.
- 15) Change the displayed text.
You can insert wildcards for variable contents anywhere in the notification text. Proceed as follows:
 - a) Place the cursor where you wish to insert the wildcard.
 - b) Select under **Placeholders** the wildcard you wish to insert.
 - c) Select **insert**.The selected wildcard is inserted in the current cursor position.
- 16) If required, select under **Included body parts** further message parts to be changed.
- 17) Click on **Show preview** to check the changed body parts in their entirety.
A sample text is displayed for inserted wildcards.

- 18) After you have changed the body parts for the selected occasion make sure that the changes are suitable for all other occasions also. Proceed as follows:
 - a) Select under **Trigger name** another occasion that uses the changed body parts.
 - b) Click on **Show preview**.
 - c) Check whether the previously made changes are suitable for this occasion.
 - d) Check the changes for the other relevant occasions also.
- 19) After you have completed all changes, click on **Save** to back up the changes.

The modified notification text will be used for the relevant e-mail notifications from now on.

6.15.8 Changing the Participant Signaling Restriction

With help of an announcement or signal tone, conference participants are notified:

- When another participant logs in to the conference.
- A logged-in participant leaves the conference.

This signaling may disturb the other conference participants, especially when the conference is held by a large number of participants and others join in belatedly. Participant signaling is therefore only active by default as long as not more than 14 participants have joined the conference. If, for example, the 15th participant dials in, the other conference participants will not be notified any more.

You can change the setting that restricts participant signaling if required.

NOTICE: This setting also limits the number of moderated-conference participants displayed in the conference control of the OpenScape clients. When this number is exceeded, only the conference's moderators and the local participant are displayed.

Start the configuration

How to configure the participant signaling restriction:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.
The configuration dialog of the conference portal plugin opens.
- 3) Switch to the Configuration tab.
The Conferences dialog opens.
- 4) Under Media configuration, select **Audio settings**.

- 5) Specify under **Number of joint participants determining suppressing of join/leave indication** the number of conference participants to disable participant notification.

Enter **11**, for example, if participant signaling is to be active up to ten participants.

- 6) Select **Save** to copy the modified setting.

You have thus changed the setting that restricts participant signaling.

6.15.9 Disabling the Full HD Resolution

Disabling the deployment of the video resolution Full HD can be useful – for example to restrict the network load. You can configure this setting individually for each OpenScape Media Server.

Start the configuration

How to disable the video resolution Full HD:

- 1) Open the following configuration file on the OpenScape Media Server computer system with a text editor:

`level-resolution.xml`

By default, you find this file in the following folder of the computer system:

`<Osc-Install27>/mediaserver/application_host/bin/res/layout`

- 2) In the configuration file, replace each text `Resolution="hd1080"` with:

`Resolution="hd720"`

- 3) Save the changes in the configuration file.
- 4) If you wish to disable the video resolution Full HD across the system, execute the described steps for each OpenScape Media Server.

As of the next video conference, communication devices cannot negotiate the video resolution Full HD with the conference portal anymore.

6.15.10 Configuring Video Layouts used

You can determine in which manner the conference portal can represent the video images of the conference participants on the device displays of the participants.

Start the configuration

How to configure the manners in which the conference portal represents the video images of the single conference participants:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

²⁷ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

- 3) Switch to the Configuration tab.

The Conferences dialog opens.

- 4) Under Media configuration, select the **Video Settings**.

The video settings dialog opens.

- 5) Select under **Layout types** the check box of the video layouts the conference portal shall offer to the conference participants for selection during a video conference.
- 6) If you select several layouts under **Layout types**, use the **Default Layout** combo box to choose the layout with which the conference portal shall start every conference.

After the conference start, each conference participant can switch the layout for all conference participants via the video menu. In this case you can select only the layouts marked under **Layout types**.

- 7) If you have selected one of the Active Speaker layouts, set under **Sensitivity level** how quickly the video image shall react to active-speaker switch-overs.

The image of the currently active speaker should react to switching the person who conducts the conversation delayed. This prevents the image of the active speaker from changing too often.

- 8) If the conference portal shall provide conference participants with user-individual video streams, select the **Individual Views On**.

You need to activate this option if conference participants shall be enabled to hide their own video image in the video display.

- 9) Select **Save** to copy the modified setting.

You have now determined in which manner the conference portal can represent the video images of the conference participants on the device displays of the participants.

6.15.10.1 Common Video View Layout

All participants will see the same video view layout.

For moderated conferences, the moderators can define what video view layout will be seen by all the participants, choosing between the Single View and Tile Based View.

For open conferences, the layout cannot be changed, and all participants will see Tile Based View.

The Common Video View Layout is deployed based on the following settings:

- Unmark the "Individual Views On" check box, in Media Configuration/Video Settings tab

- Add the following setting in WebClientUI.cfg:
VideoLayout - Should reflect the CMP configuration
temp.personalVideoLayout = false

With the Common Video Layout, depending on CPU server capacity, the tile based layout shall be able to support up to 49 video streams, growing dynamically from 1 video, to 2x2, 3x3, 4x4, 5x5, 6x6 and 7x7 videos.

To grow up to 49 tiles, it is required to have the following entry in ConferencingApplication.application.xml

<allowLayoutForMaxParticipants>true</allowLayoutForMaxParticipants>

6.15.11 Configuring Mailbox Recognition of the Conference Portal

NOTICE: You need to execute the configuration steps of this chapter only if you use OpenScape Voice as directly connected communications system. This feature will otherwise not be supported.

Before the conference portal connects a call to a conference it will check whether the associated connection partner is a voicemail system. If this is the case, the conference portal terminates the call and does not connect it to the conference.

Start the configuration

How to configure the conference portal for it to suppress connections to the voicemail system:

- 1) You have already created one end point for each connected OpenScape Media Server in OpenScape Voice. Configure the **Full** setting for the **SIP Privacy Support** flag in all associated end point profiles in OpenScape Voice.

This will signal the addresses for reroutings by means of SIP.

- 2) Check that the UC Application users have been assigned the forward access number of the voicemail system used by means of the custom voicemail number.

NOTICE: The voicemail number must have been specified in the Global Number Format (GNF).

- If you use the voice portal as voicemail system then you should have configured this in the following section:
[Configuring a Voicemail Number for Users](#)
- If you use OpenScape Xpressions as voicemail system then you should have configured this in the following section:
[Configuring Voicemail Numbers for Users](#)

6.15.12 Managing Video Layouts for Conferences

Experts can use configuration files to adjust the layouts that the conference portal uses for video conferences.

[Concept of Managing Video Layouts](#) describes details of managing the video layouts.

6.15.13 Managing Conferences independently of OpenScape UC Application

OpenScape UC Application is shipped with the conference management tool Coman. You can use this tool to manage conferences of the conference portal independently of OpenScape UC Application via command line or a conference table.

[Conference Management Tool Coman](#) describes details about the conference management tool Coman.

6.16 Managing the OpenScape Media Server

Managing the OpenScape Media Server is described in the *OpenScape Media Server Administrator Manual*.

6.17 Managing OpenScape Web Client (Webserver Components)

This chapter provides information about the following topics:

- [Changing the HTTP / HTTPS Port for OpenScape Web Client](#)
- [Changing the OpenScape Web Client used by default](#)
- [Enabling the Display of non UC Users Name in Call Control and Journal](#)
- [Enabling the Location Fields in the Web Client](#)
- [Enabling the Download of the OpenScape Desktop Integration Tool](#)
- [Specifying the Synchronization Strategy for Contact Details](#)
- [Scheduling the Synchronization of Private Contact Details](#)
- [WebClient UI Customization](#)
- [Browsers and Language](#)
- [Import of contact data from other sources](#)
- [Configuration for Team : Team shall take my calls](#)
- [Browsers and Web Sockets](#)
- [Limit the entries in UC Journal / Call History](#)
- [Reduced Set of presence states](#)
- [Enable Voicemail tab for Settings](#)
- [Reducing size of recorded audio files](#)
- [Modification of Content-Security-Policy](#)
- [Handling Profile Rules](#)

IMPORTANT: In UC Conferencing, using the recording functionality in Web-Only conferences will break the Web-Only definition. This is because Media Server does not provide recording functionality through the FastviewerApplet.

6.17.1 Changing the HTTP / HTTPS Port for OpenScape Web Client

The OpenScape Web Client uses the following ports for HTTP or HTTPS by default:

- Port 7789 for HTTP
- Port 8443 for HTTPS

You can change these ports if required. For this, you need to configure a port forwarding.

NOTICE: If you have not configured the port modification using the recommended port forwarding, the log file `errors-WebtierController*.log` of the OpenScape Web Client displays the following entry: `java.net.SocketException: Permission denied`

NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
 - SLES 15 SP5, for UC V11R6
-

Start the configuration for SLES 12

How to configure a port forwarding for the default HTTP or HTTPS port of the OpenScape Web Client:

The steps are:

```
# cd /etc/wicked/extensions
# mv firewall firewall.sample
```

create the following script with vi

```
#!/bin/bash
scriptdir=$(dirname $0)
if [ -f "$scriptdir/functions" ]; then
    . "$scriptdir/functions"
fi

command=$1
shift

case $command in
up)
    if [[ $WICKED_INTERFACE_NAME != "lo" ]]; then
```

```

        /usr/sbin/iptables -A FORWARD -i $WICKED_INTERFACE_NAME
        -p tcp --dport <PORT> -j ACCEPT
        /usr/sbin/iptables -t nat -A PREROUTING -i
        $WICKED_INTERFACE_NAME -p tcp --dport <PORT> -j DNAT --to-
        destination :<default port>
    fi
;; down)
    if [[ $WICKED_INTERFACE_NAME != "lo" ]]; then
        /usr/sbin/iptables -D FORWARD -i
        $WICKED_INTERFACE_NAME -p tcp --dport <PORT> -j ACCEPT

        /usr/sbin/iptables -t nat -D PREROUTING -i
        $WICKED_INTERFACE_NAME -p tcp --dport <PORT> -j DNAT --to-
        destination :<default port>
    fi
;; *)
    wicked_error "Unsupported script action $command"
;;
esac
exit

```

Replace the expression <Port > with the port number you wish to use for the OpenScope Web Client – e. g. 443. and The expression <Default Port > with the port number the OpenScope Web Client uses by default – thus either 7789 for HTTP or 8443 for HTTPS Save it under /etc/wicked/extensions/ with the name HiPathCAPortForwarding

Make HiPathCAPortForwarding executable and create a symbolic link to HiPathCAPortForwarding with the following commands

```

# chmod +x HiPathCAPortForwarding
# ln -sf /etc/wicked/extensions/HiPathCAPortForwarding/etc/
wicked/extensions/firewall

```

In order for the new settings to take effect, restart the network or reboot the server.

6.17.2 Enabling the Display of non UC Users Name in Call Control and Journal

When a system administrator enables this feature, the names of non UC users, provided by the PBX will be displayed in the Call Control and Journal of the OpenScope Web Client.

How to enable the display of non UC users name in Call Control and Journal:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install²⁸>/HiPathCA/config/common/

- 2) Set the value of the property ShowPbxDisplayNames to true to enable the feature. The default value is false.

²⁸ <Osc-Install > is the setup directory of OpenScope UC Application: /opt/siemens/ respectively /enterprise/

- 3) Save the changes in the configuration file.

The names of non UC users provided by the PBX will be displayed in the Call Control and Journal of the OpenScape Web Client.

6.17.3 Enabling special keys used by WebClient regarding incoming calls

When a system administrator enables this feature, the options/keys regarding numbers for specific scenarios of incoming calls will be displayed in the Call Control and Journal of the OpenScape Web Client.

How to enable the display options/keys regarding incoming calls

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install²⁹>/HiPathCA/config/common/

- 2) Set the value of the property:

- ShowPbxDisplayNumber to true to enable the PBX number display feature. When set to true, the number provided by the PBX will be displayed in case the normalized number is not available.
- ShowPbxMLHGPilotNumber to true to enable the MLHG number feature. When set to true, the MLHG number provided by the PBX will be displayed in an incoming call

- 3) Save the changes in the configuration file.

IMPORTANT: The option ShowPbxMLHGPilotNumber should NOT be enabled when ShowPbxDisplayNumber is already enabled in the system.

6.17.4 Enabling the Location Fields in the Web Client

When a system administrator enables this feature, the location-based fields, such as Location, Building and Room, as well as the free text field Note appear in the Contact Details and in the Advanced Search of the OpenScape Web Client.

How to enable location search:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install³⁰>/HiPathCA/config/common/

²⁹ <Osc-Install > is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

³⁰ <Osc-Install > is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

- 2) Set the value of the following properties to true (depending on the configuration requirements). The default value is false:

Contact.Location

Contact.Room

Contact.Building

Contact.Note

- 3) Save the changes in the configuration file.
- 4) Execute the following command on the application computer to restart the relevant web server component.

```
/etc/init.d/symphoniad restart WebClient_BE
```

The relevant web server component stops and immediately reboots again. The new setting will thus take effect on the application computer.

The fields Location, Building and Room and the free text field Note will be displayed in the Contact Details of the OpenScape Web Client. The fields Location, Building and Room will be displayed in the Advanced Search of the OpenScape Web Client.

6.17.5 Enabling the Download of the OpenScape Desktop Integration Tool

OpenScape users can download the OpenScape Desktop Integration tool via the settings menu of the OpenScape Web Client. This feature is disabled by default.

NOTICE: Fusion for Office is preferred.

How to enable the download of the OpenScape Desktop Integration tool:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install³¹>/HiPathCA/config/common/

- 2) Set the value of the property DIDownload to true to enable the feature. The default value is false.
- 3) Save the changes in the configuration file.

The download of the OpenScape Desktop Integration tool has been enabled. OpenScape users will not view the option of downloading the OpenScape Desktop Integration tool from the settings menu of the OpenScape Web Client.

NOTICE: When a system administrator enables or disables the download of the OpenScape Desktop Integration tool, OpenScape users can view the changes by manually refreshing the OpenScape Web Client page or by logging off and on again to the OpenScape Web Client.

³¹ <Osc-Install > is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

6.17.6 Specifying the Synchronization Strategy for Contact Details

Users can edit information related to contacts from server directories, such as telephone numbers and e-mail addresses. According to the configuration set, when a user selects to synchronize the contact details with the server directory on the OpenScape Web Client interface, either all fields will be synchronized and user modified data will be kept in case of empty directory fields (default setting), or only empty user modified fields will be synchronized and fields that were cleared by the user will be overwritten with directory data during synchronization.

How to select the synchronization strategy for contact details:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on Show next to Actions - Services Status.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Search the list for the **Contactservice** component and click on the associated component name.

The dialog with the contact service settings opens.

- 6) Specify one of the following values in the **Synchronize Strategy** field.

Value	Description of the value for the contact service status
0	OpenScape users are not allowed to modify any fields.
1	Synchronize all fields.
2	Synchronize only empty user modified fields, i.e. fields which got cleared from a user are overwritten with directory data during synchronization
3	Synchronize all fields, but keep user modified data in case of empty information from the server directory. This is the default setting.

- 7) Click Save.

6.17.7 Scheduling the Synchronization of Private Contact Details

Details of private contacts who are linked by the SourceId attribute to a public contact in the Global Contact List can be automatically synchronized. The

automatic synchronization can be scheduled to be performed once a day or even continuously.

The following configuration options are available in the instance file properties:

Table 12: Synchronization configuration options

Property name	Description	Default value
SynchronizeStrategy	Values: 0: OpenScape users are not allowed to modify any fields. 1: Synchronize all fields 2: Synchronize only empty user modified fields, i.e. fields which got cleared from a user are overwritten with directory data during synchronization 3: Synchronize all fields, but keep user modified data in case of empty information from the server directory.	3
SynchronizeStrategyExcludeFields	A list of field names which are not considered for the sync	
SynchronizeStrategyOverrideEnable	enable/disable the "SynchronizeStrategyOverride" Value = true / false	false
SynchronizeStrategyOverride	See SynchronizeStrategy	3
SynchronizeStrategyExcludeFieldsOverrideEnable	enable/disable the "SynchronizeStrategyExcludeFieldsOverride" Value = true / false	false
SynchronizeStrategyExcludeFieldsOverride	SynchronizeStrategyExcludeFields	
SynchronizeSchedulerStarted	Starts or stops the synchronization scheduler. If stopped no trigger will fire and therefore no contact will be synchronized Value = true / false	false
MinutesToIgnoreRepeatedSyncRequest	value = positive number / minutes The value given is a time in minutes. In this time a subsequent request to synchronize a single contact is rejected. A value of "0" means that the feature is disabled. This feature is meant to reduce database load by preventing that the same contact is synchronized too often. The lower the value the better the responsiveness, but the higher the database load.	60

Property name	Description	Default value
SchedSyncTriggerDefs	value ::= "" trigger_definition, {";", trigger_definition} trigger_definition ::= cron_expression, " ", trigger_name, " ", load_factor, " ", sleep_time cron_expression = This expression defines when and how often the trigger fires. See CronTrigger Tutorial. trigger_name = This is the Name of the trigger. It needs to be unique. load_factor = Since the smallest repeat interval for a cron-trigger is 1 sec, you can define with this value how many entries of the sync queue should be processed with one run of the sync job. sleep_time = This parameter is given in milliseconds and defines the interval between the processing of sync queue entries within one run of the sync job. In general this parameter should be adjusted in a way that the sync job finishes before the associated trigger fires again. With this parameter you define when and how many contacts are sync'ed.	* * 19-23 * * ? Nightly S 20 50;* * * * ? Daily S 200
SchedCleanTriggerDefs	value ::= "" trigger_definition, {";", trigger_definition} trigger_definition ::= cron_expression, " ", trigger_name cron_expression = s.a. trigger_name = s.a. The clean job optimizes internal queue data structures to reduce the memory footprint.	0 0 * * * ? Hourly Clean
SchedSyncPublicConnectors	value ::= connector_responsibility, {";", connector_responsibility} connector_responsibility = The definition is found in the instance file. With this parameter you can limit the synchronization to a subset of the available public connectors. Especially LDAP connectors might be overstrained by the sync.	svc-globalcontactlist

Property name	Description	Default value
SchedSyncQueueLimit	value = positive number This is the max number of entries in the synchronization queue at any one time. Violating this limit will result in contacts not being synchronized. It is highly desirable that this queue size is not reached, as this means a large memory consumption.	1000000
org.quartz.?	Do not change this without request by Development. These settings cannot be applied dynamically. Writable property should be set to 'false', if these settings are introduced to the instance file. That means the settings cannot be changed via CMP.	<Property name="org.quartz.schedulerName" value="org.quartz.schedulerName" writable="false"/> <Property name="org.quartz.schedulerName" value="org.quartz.schedulerName" writable="false"/> <Property name="org.quartz.schedulerName" value="org.quartz.schedulerName" writable="false"/> <Property name="org.quartz.schedulerName" value="org.quartz.schedulerName" writable="false"/> <Property name="org.quartz.schedulerName" value="org.quartz.schedulerName" writable="false"/>

CronTrigger

CronTrigger uses "cron expressions", which are able to create firing schedules such as: "At 8:00am every Monday through Friday" or "At 1:30am every last Friday of the month".

A cron expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field.

So cron expressions can be as simple, such as: * * * * ? *

or more complex, such as : 0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2002-2010

Cron Expressions:

Table 13: Cron expressions

Field Name	Mandatory	Allowed Values	Allowed Special Characters
Seconds	YES	0-59	, - * /
Minutes	YES	0-59	, - * /
Hours	YES	0-23	, - * /
Day of month	YES	1-31	, - * ? / L W

Field Name	Mandatory	Allowed Values	Allowed Special Characters
Month	YES	1-12 or JAN-DEC	, - * /
Day of week	YES	1-7 or SUN-SAT	, - * ? / L #
Year	NO	empty, 1970-2099	, - * /

Table 14: Special characters

* ("all values")	Used to select all values within a field. For example, "" in the minute field means "every minute".
? ("no specific value")	Useful when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, if I want my trigger to fire on a particular day of the month (say, the 10th), but don't care what day of the week that happens to be, I would put "10" in the day-of-month field, and "?" in the day-of-week field. See the examples below for clarification.
- -	Used to specify ranges. For example, "10-12" in the hour field means "the hours 10, 11 and 12".
, -	Used to specify additional values. For example, "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday"
/ -	Used to specify increments. For example, "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". You can also specify '/' after the " character - in this case " is equivalent to having '0' before the '/'. '1/3' in the day-of-month field means "fire every 3 days starting on the first day of the month"
L ("last") -	Has different meaning in each of the two fields in which it is allowed. For example, the value "L" in the day-of-month field means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing results.

W ("weekday") -	Used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.
# -	Used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means "the third Friday of the month" (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month.

NOTICE: The legal characters and the names of months and days of the week are not case sensitive. MON is the same as mon.

NOTICE: The 'L' and 'W' characters can also be combined in the day-of-month field to yield 'LW', which translates to "last weekday of the month".

Examples

Table 15: CronTrigger examples

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 15 10 * * ?	Fire at 10:15am every day
0 15 10 * * ? *	Fire at 10:15am every day
0 15 10 * * ? 2005	Fire at 10:15am every day during the year 2005
0 * 14 * * ?	Fire every minute starting at 2pm and ending at 2:59pm, every day

Expression	Meaning
0 0/5 14 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day
0 0/5 14,18 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day
0 0-5 14 * * ?	Fire every minute starting at 2pm and ending at 2:05pm, every day
0 10,44 14 ? 3 WED	Fire at 2:10pm and at 2:44pm every Wednesday in the month of March.
0 15 10 ? * MON-FRI	Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
0 15 10 15 * ?	Fire at 10:15am on the 15th day of every month
0 15 10 L * ?	Fire at 10:15am on the last day of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L 2002-2005	Fire at 10:15am on every last friday of every month during the years 2002, 2003, 2004 and 2005
0 15 10 ? * 6#3	Fire at 10:15am on the third Friday of every month
0 0 12 1/5 * ?	Fire at 12pm (noon) every 5 days every month, starting on the first day of the month.
0 11 11 11 11 ?	Fire every November 11th at 11:11am.

NOTICE: Pay attention to the effects of '?' and '*' in the day-of-week and day-of-month fields.

Keywords for the Attribute Exclusion Lists

Table 16: Keywords for the attribute exclusion list

Phone fields	"phone_business_1" "phone_business_1_normalized" "phone_business_2" "phone_business_2_normalized" "phone_home_1" "phone_home_1_normalized" "phone_mobile_1" "phone_mobile_1_normalized" "phone_video_1" "phone_video_1_normalized"
Fax fields	"fax_business_1" "fax_business_1_normalized"
E-mail fields	"email_1" "email_1_normalized" "email_2" "email_2_normalized"
Address fields	"addr_building_number_1" "addr_city_1" "addr_company_name_1" "addr_country_code_1" "addr_department_1" "addr_postal_code_1" "addr_room_number_1" "addr_state_or_province_1" "addr_street_1" "addr_url_1"

System management for the components of OpenScape UC Application

Common fields	"alias" "description" "display_name" "external_source_id" "gender" "given_name" "im_address" "last_name" "middle_name" "notice" "object_class" "picture" "salutation" "title" "vanity_code" "sounds_like"
Client Matter Codes	"client_matter_code_1" "client_matter_code_2" "client_matter_code_3" "client_matter_code_4" "client_matter_code_5" "client_matter_code_6"
Custom Fields	"custom_1" "custom_2" "custom_3" "custom_4" "custom_5" "custom_6"
Technical Fields	"contact_sym_identity"
Always excluded from the sync	"owner_sym_identity" "source_id" "contact_id" "presence_info"

6.17.8 WebClient UI Customization

It is possible to customise the User Interface of the UC WebClient, such as the following User Interface elements:

- logo of the UC application
- colors of the WebClient User Interface
- colors of the WebClient icons

However, this should be only done by Professional Services and Solutions (PS & S) of Unify Software and Solutions GmbH & Co. KG.

In order to see what is supported and what needs to be changed, please check the ReadMe.txt file located under <OSC-Install³²>/HiPathCA/WebSpace/Portal/webapps/openscapeuc/resources/branding/.

6.17.9 Browsers and Language

Each browser is using a different logic / source to investigate the user's language.

- Internet Explorer (11) uses the regional setting in control panel which also define date format and currency for the OS (regardless of the language configured in Internet Explorer settings).
- Firefox uses the language defined in the language list in the browser setting.
- Chrome uses the language of the Chrome UI (regardless of the language list in Chrome settings).

A customer still can reenable the language switcher in WebClientUI.cfg => ShowLanguageSwitch but should know that this could have a serious impact on performance and memory consumption of the browser.

NOTICE: WebClientUI.cfg is located under <OSC-Install³³>/HiPathCA/config/common

6.17.10 Import of contact data from other sources

In some cases it is necessary to adapt the import / export configuration, e.g. to avoid problems with an older specification or just to speed up the import / export process.

Consider the following:

- Backup the existing configuration file: tw_osc_utf_8.cfg

³² <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

³³ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

- Adapt the existing configuration file in the following folder, according to your requirements:

installationfolder>/config/services/default/AddressService\imp_exp

Example:

The admin can use the available templates and adjust the configuration file according to customer's needs. For this, in an Outlook / Exchange environment, the contents of the outlook_en.cfg file must be copied into the tw_osc_utf_8.cfg file.

IMPORTANT: Depending on the user's local settings, the proper "outlook_xx.cfg" file must be used, where "xx" represents the language to be used (e.g. "de" for German or "en" for English).

A reboot of the webclient is required for the changes in the configuration to take effect.

6.17.11 Configuration for Team : Team shall take my calls

Since V9R2 a new system wide configuration parameter TeamShallTakeMyCallsDefault has been introduced.

When an invitation to Team is received there is a feature "Team shall take my calls" which can be activated via enabling the checkbox "Team shall take my calls" from the communication options. Up to now the user has to enable this explicitly. The new configuration parameter defines the default behavior: When the parameter TeamShallTakeMyCallsDefault is set to true, then the checkbox for "Team shall take my calls" is enabled by default. In this case, if a user does not want this feature then this user can disable this setting by unchecking the checkbox "Team shall take my calls" explicitly. In case the configuration parameter TeamShallTakeMyCallsDefault is not defined, then it is the same as this configuration parameter is set to false. The default setting for TeamShallTakeMyCallsDefault is false, so that the default behavior for the Team invitation does not change, meaning that if the user wants the feature "Team shall take my calls" then the user must enable it explicitly.

In short:

- configuration parameter TeamShallTakeMyCallsDefault is set to true: The feature "Team shall take my calls" is enabled by default.
- configuration parameter TeamShallTakeMyCallsDefault is set to false: The feature "Team shall take my calls" is disabled by default.

This configuration parameter can be set in file WebClientUI.cfg.

It is under <OSC-Install³⁴>/HiPathCA/config/common/

The default value is false (same behaviour as not setting it)

```
# # You can set systemwide the default option
of the "property" team shall take my calls #
TeamShallTakeMyCallsDefault = false
```

³⁴ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

6.17.12 Browsers and Web Sockets

The Web Socket must be enabled in the browser which is used to access the UC Web Client. If the Web Socket is not enabled the Web Client will not be fully functional. Some features like eventing will not work.

Normally Web Sockets are enabled by default in the supported browsers. See also <https://en.wikipedia.org/wiki/WebSocket>.

6.17.13 Enabling the Set all read button in Call History

You can use the Set all read button to mark all calls in the Call History as read.

Follow the steps below to enable this feature:

- 1) Open the following configuration file with a text editor:

`WebClientUI.cfg`

This file is located under: `<Osc-Install35>/HiPathCA/config/common`

- 2) Set the value of the `callHistory.markAllCallsAsRead` parameter to true to enable the feature.

```
callHistory.markAllCallsAsRead = true
```

The default value is false.

When set to true, the Set all read button is displayed in the Call History tab of OpenScape UC WebClient.

- 3) Save the changes in the configuration file and restart the OpenScape UC WebClient.

6.17.14 Limit the entries in UC Journal / Call History

It is possible to set a maximum number for the entries in the Journal (Call History) and also for how long the entries are kept in the history.

It is defined in file `JrnService.cfg`.

The file is located under

`<Osc-Install36>/HiPathCA/config/services/default/JrnService`

There is the parameter for setting the limit on entries in the Call History:

```
journalLimitEntries = <value>
```

If the value is set to 0 or the entry is not set at all then the number of Entries is unlimited.

There is the parameter to define how long this entries are kept in the history.

```
journalLimitDays = <value>
```

You define here the number of days, e.g. if you want one week, then define 7 if you want two weeks then define 14.

³⁵ <Osc-Install > is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

³⁶ <Osc-Install > is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

If the value is set to 0 or the entry is not set at all then the entries will not be deleted. In any other case the entries will be removed when they are older as the defined value.

6.17.15 Reduced Set of presence states

It is possible to use less presence states

IMPORTANT: A project-specific release is required to activate this feature.

It is configurable in "WebClientServlet.cfg" which is in path <Osc-Install³⁷>/HiPathCA/config/common.

Define the available presence states under AvailablePresenceStates

e.g. AvailablePresenceStates = active, away, busy

Possible values and presence states:

- active -> AVAILABLE
- away -> AWAY
- autoAway -> BE RIGHT BACK
- busy -> BUSY
- dnd -> DO NOT DISTURB
- meeting -> IN MEETING

The following restrictions apply:

- AWAY, AVAILABLE and BUSY are mandatory in the presence status .
- This feature is not backward compatible to old fusion4office versions it will work only for Fusion for Office / Fusion for Notes V1R6.46.25 or newer.
- UCMA deployment is not compatible with this feature
- Local presence sync (deployment mode = Microsoft OCS) is not compatible with this feature.
- Automatic presence change to "Be right Back" will not work if the "Be right back" presence status is removed (screen saver, lock screen and sleep/hibernate mode will not change the presence status)
- Automatic presence change to "In a meeting" will not work if the "In a Meeting" presence status is removed (calendar appointment or meeting "Show as" "Busy" will not change the Fusion for Office / Notes presence status anymore)

6.17.16 Enable Voicemail tab for Settings

In V11, the voicemail tab can be enabled which allows the user to record greetings for the voicemail box, so for calls redirected to the voicemail box the caller gets an appropriate greeting.

The feature is described in the UC WebClient User Guide.

³⁷ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

In the file `WebClientUI.cfg` under `<Osc-Install38>/HiPathCA/config/common`

Update the configuration file as follows:

```
#  
# Set this entry to 'true' to use the new, simplified  
# Voicemail settings UI; otherwise, the old Xpressions link  
# is displayed  
#  
UseNewVmSettings = true
```

After the setting of the parameter has been applied the OSC UC Server has to be restarted to this parameter to take effect.

“Clear browsing data” should be done in the Webrowsers or a webpage refresh to this configuration takes effect in the WebClient

6.17.17 Reducing size of recorded audio files

In V11 it is possible to reduce the size of recorded wav files for your recorded greetings.

Browsers typically record audio at 48000 samples/second, which is very high compared to the actual quality needs. Downsampling can reduce the audio files' size without effecting the perceived quality of the voice

Downsampling is actually achieved by skipping frames of the recorded audio when saving (decimation).

To reduce size you can use the following parameters `RecordInStereo` and `TargetSampleRate` that exist in the `WebClientUI.cfg` file which are by default set to 'false'.

In the file `WebClientUI.cfg` under `<Osc-Install39>/HiPathCA/config/common`

Update the configuration file as follows:

```
#  
#Set this entry to 'true' to record stereo audio for  
# voicemail greetings.  
# Default is 'false' (mono)  
#  
RecordInStereo = true  
and:  
# For example, if the browser records audio at 48000 and the  
# TargetSampleRate is set to 12200, the actual audio sample rate will be 16000  
# If the browser native sample rate is lower that this value, this parameter is  
# ignored (upsampling not supported)
```

³⁸ `<Osc-Install >` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

³⁹ `<Osc-Install >` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

Default is 0 (downsampling disabled)

#

TargetSampleRate = 12000

The actual final sample rate will be a number like $\text{BrowserSampleRate}/N$, where N is a positive integer. If your browser records at 48000Hz and you type TargetSampleRate = 12200, your sample rate will actually be 16000 ($48000/3$)

After the setting of the parameter has been applied the OSC UC Server has to be restarted to this parameter to take effect.

“Clear browsing data” should be done in the Web browsers or a webpage refresh to this configuration takes effect in the WebClient

6.17.18 Handling Profile Rules

Profiles are used to handle rules so e.g. to define scenarios for meetings, business trips, etc. In case there is already a profile active, you can select another profile. In this case the profile you clicked on is getting activated.

With a profile you can define a presence state, assign one or more rules which are applied, when the profile is active and set a hierarchy of the rules when the profile is active.

IMPORTANT: Only one profile can be at a time active

IMPORTANT: The profiles SmartClient rules and Standard Profile are automatic profiles created for imported rules, when you migrate from previous versions. If you unassign the rules associated with these profiles, the profiles will be automatically hidden and not be available any more.

6.17.19 Display the second e-mail (home e-mail)

OpenScape Web Client contacts normally display both the Work and Home e-mail addresses. However you can enable or disable your Home e-mail field display for certain contacts e.g. LDAP Connector contacts.

To configure this, please follow the steps below:

How to enable / disable the feature:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install1>/HiPathCA/config/common/1

- 2) Set the value of the property AttrMap.mail2 to true to enable the feature, or to false to disable it. The default value is true.
- 3) Save the changes in the configuration file.

NOTICE: Enabling this attribute does not enable the second email when creating a new private contact. It only applies to just your existing contacts.

NOTICE: When a system administrator enables or disables this feature, OpenScape users can view the changes by manually refreshing the OpenScape Web Client page or by logging out and in again to the OpenScape Web Client, or when the automatic synchronization takes place (once a day or according to the configuration set by the administrator).

1 <Osc-Install> is the setup directory of OpenScape UC Application:
/opt/siemens/ respectively /enterprise/
=

6.17.20 Hide the WebRTC Guest Access button in UC Conferences

OpenScape UC offers the possibility to hide the “Join as a guest” button in case the UC server is not using WebRTC (system is WebRTC enabled). You can also hide the Guest Access button even if the system is WebRTC enabled.

How to hide Guest Access button:

- 1) Modify the WebRTC Service instance file in the file system with a text editor. You can find this file under:
/opt/siemens/common/conf/config-beans
- 2) Set the value of property GuestAccessEnabled to false. The default value is true.
- 3) Save the changes in the configuration file.
- 4) Restart your system for the changes to take effect.

NOTICE: You can also do this via CMP (by navigating to the properties section of the “WebRTC Service”). The value of this property is “true” by default, meaning that WebRTC guest access will be enabled by default for a WebRTC enabled system. Change it to “false”. Please note that apart from the value defined for this attribute, this method will return false if WebRTC feature is not installed for the system.

NOTICE: If you modify the GuestAccessEnabled property via CMP it is not required to restart your system.

6.17.21 Changing the Authentication Cookie Management Policy

OpenScape UC uses a Cookie named OpenScapeUC as a login/authentication token and it is initialized after a successful login. This cookie makes it possible for the user to avoid reentering the user credentials multiple times if he has already performed a successful login recently.

It is possible to configure the handling of these tokens to be more restrictive by retaining their revocation status in the context of the application. The user is then able to add a token to the revoked token list by performing a manual logout, so that it is impossible for someone to reuse the same authentication token.

In order to enable this functionality you will have to modify the file `WebClientServlet.cfg` under:

```
<Osc-Install>/HiPathCA/config/common/
```

and set the property `OpenScapeUC.PersistState` to `true` and restart UC.

```
OpenScapeUC.PersistState = true
```

This functionality is disabled by default, so the default value of the property is `false`.

IMPORTANT: If you change the value of this property all the active authentication cookies of the users that were issued with the previous settings will be invalidated. So the users will have to perform a manual login the first time they use OpenScape UC after the configuration changes.

6.17.22 Configuration for SIP DNS SRV

Starting with UC V11 R3, it is possible to configure the SIP DNS SRV mechanism for WebRTC. In order to configure it you have to modify the file `WebClientServlet.cfg` under:

```
<Osc-Install>/HiPathCA/config/common/
```

Set the property `SipDnsSrvFqdn` with the fully-qualified domain name (fqdn) of the SIP DNS SRV. By default this property is empty which means that the retrieved SIP IP from OSV will be used for the WebRTC account registration.

If this property is defined then this will be sent instead of the SIP IP and the SIP port will be set to 0.

6.17.23 Display the Emergency Call Disclaimer

OpenScape UC Clients should not be used to make emergency calls. Doing so might result in the call not being routed properly to the emergency service provider or incorrect location information being provided. If you need to make an emergency call, please use a land line or mobile phone.

A disclaimer message screen can be displayed to users in order to inform them about this restriction. This can be configured via the `WebClientUI.cfg` settings.

If the feature is enabled, the disclaimer will be displayed every time during login until the user clicks `Accept`.

To configure this, please follow the steps below:

How to enable / disable the feature:

- 1) Open the following configuration file with a text editor:

WebClientUI.cfg

You can find this file in the following folder of the application computer:

<OSC-Install1>/HiPathCA/config/common/1

- 2) Set the value of the property emergencyCallsDisclaimer to true to enable the feature, or to false to disable it. The default value is false.
- 3) Save the changes in the configuration file.

6.17.24 Modification of Content-Security-Policy

Starting with UC 10.3.7.0 it is possible to modify the value of the Content-Security-Policy header for OpenScapeUC UI. The user can update the default value of this header by adding new domains. The default value of this header is "frame-ancestors teams.microsoft.com *.teams.microsoft.com *".

In order to modify this header the user will have to edit the following file in each FE node (or in the unique node if it's a small deployment) :

<Osc-Install>/HiPathCA/config/deployment.props

The property that is responsible for this functionality is named UC_CONTENT_SECURITY_POLICY_ADDITIONAL

The system has to be restarted in order to activate the changes.

6.18 Managing the Facade Server

This chapter provides information about the following topics:

- [Concept of the Facade Server Management](#)
- [Configuring the Facade Server](#)
- [Activating SSL for Facade Servers](#)

6.18.1 Concept of the Facade Server Management

OpenScape UC Application must be connected to the internet via a so-called Facade server so that the OpenScape Mobile Client can communicate with OpenScape UC Application. This Facade server is an application server that serves as endpoint for the inbound internet connections of the OpenScape Mobile Clients.

You define the Facade server settings in the facade.properties property file. You find this file in the following folder of the computer system on which the Facade server is installed.

Windows system

C:\Program Files\<setup directory of the Tomcat server>

Linux system

/usr/local/facade/<setup directory of the Tomcat server>

Modifications to the property file do not take effect until the Tomcat server has been rebooted.

IMPORTANT: When the Tomcat server is stopped, the connections to the OpenScape Mobile Client are disrupted. The relevant users need not log in again after a Tomcat server reboot.

The following settings can be configured in the property file for the Facade server:

- [https](#)
- [logFile](#)
- [maxLogFileSize](#)
- [serverAddress](#)
- [serverName](#)
- [serverPort](#)
- [symphoniaCallTimeout](#)
- [traceLevel](#)
- [useAddressTranslation](#)

These settings have the following functions.

- **https**

Possible values:	– true – activates HTTPS. – false – activates HTTP.
Default setting:	true
Associated settings:	serverPort

Defines whether Facade server and SOAP connector of OpenScape UC Application communicate via the HTTP protocol (unsecured via port 4708) or HTTPS (secured via port 4709).

If you modify this settings you need to adjust the value of the [serverPort](#) setting accordingly.

- **logFile**

Possible values:	<i><File name with suffix ></i>
Default setting:	log.txt

Defines the name of the files in which the Facade server stores logging information. The Facade server uses altogether a maximum of ten files to store logging information. These files carry names of the following format:

log0.txt to log9.txt

The Facade server describes these files in the Round-Robin procedure.

Which logging information the Facade server stores is defined in the [traceLevel](#) setting. The maximum size of these files is defined by the [maxLogFileSize](#) setting.

- **maxLogFileSize**

Possible values:	<i><Data amount in byte ></i>

Default setting:	2 000 000

Defines the size that the files in which the Facade server stores logging information may adopt.

- **serverAddress**

Possible values:	– <i><IP address></i> – <i><URL></i>
Default setting:	10.1.10.1

Defines the IP address or the URL under which the application computer of OpenScape UC Application can be reached. The Facade server connects to the SOAP connector of OpenScape UC Application under this address.

- **serverName**

Possible values:	<i><fully qualified host name></i>
Default setting:	–

Defines the fully qualified domain name under which the front-end services of OpenScape UC Application can be reached.

This specification is particularly required when NAT shall be used for the SOAP communication of the Facade server on the basis of NAT mapping tables in the `system.xml` file. See also [Configuring the Load Balancer for Front-End Computers](#).

- **serverPort**

Possible values:	<i><Protocol port></i>
Default setting:	4709
Associated settings:	https

Defines the number of the protocol port via which the Facade server communicates with the SOAP connector of OpenScape UC Application.

- **symphoniaCallTimeout**

Possible values:	<i><Time in seconds></i>
Default setting:	20

If the Facade server does not receive an answer from the SOAP connector to its connection request in the time specified here, it aborts the connection attempt. Subsequently, it sends a corresponding time-out message to the relevant OpenScape Mobile Client.

This mechanism is required as the connection requests of an OpenScape Mobile Client are processed sequentially, which limits the maximum waiting time for a connection request. If the average time for a connection setup ranges within the default setting, the value of this setting can be increased.

- **traceLevel**

Possible values:	Comma-separated list of the following values: – Call – Beginning and end of any connection – Exception – All exceptional events – User – User information – Info – Generic System information – Debug – Debug information – All – All described information
Default setting:	call,user,exception

Defines which logging information the Facade server stores.

- **useAddressTranslation**

Possible values:	– true – Phone numbers are normalized. – false – Phone numbers are dialed directly.
Default setting:	true

After the Facade server has received a phone number from an OpenScape Mobile Client for the connection setup, it may react in the following ways:

- It establishes the connection directly with the received phone number.
- It sends the received phone number first to the address translation service by OpenScape UC Application. This service normalizes the phone number and returns it to the Facade server. The Facade server then uses the normalized phone to set up the connection.

[useAddressTranslation](#) defines in which way the Facade server reacts.

6.18.2 Configuring the Facade Server

The Facade server is configured via the `properties.ini` property file.

Please refer to [Concept of the Facade Server Management](#) on page 501 to see which default settings are configured for the Facade server.

Start the configuration

How to change the Facade server settings:

- 1) Open the following Property file with a text editor:

`properties.ini`

You find this file in the following folder of the computer system on which the Facade server is installed.

Windows system `C:\Program Files\<setup directory of the Tomcat server>`

Linux system `/usr/local/facade/<setup directory of the Tomcat server>`

- 2) Adjust the desired settings in the Property file.

- 3) Save the changes in the Property file.

IMPORTANT: The Tomcat server is stopped by the following step. This disrupts the existing connections to OpenScape Mobile Clients.

- 4) Reboot the Tomcat server to activate the modifications.

You have now changed the Facade server settings and activated the modifications by a Tomcat server reboot.

6.18.3 Activating SSL for Facade Servers

The Facade server communicates with the UC Application application computer within the company's own network and with the OpenScape Mobile Clients via internet. The Facade server can use SSL for this communication.

How to activate SSL for the Facade server is described in the *OpenScape UC Application, Installation and Upgrade* manual.

The Facade server uses certificates supplied as standard after the installation. How to configure individual certificates for SSL-based communication in the Facade server describes [Configuring a Certificate Strategy](#).

6.19 Managing the Openfire Server

This chapter provides information about the following topics:

- [Resynchronization of the Presence Access Privileges in a networked UC Application Environment with several Openfire Servers](#)
- [Changing the Openfire Server Certificates](#)
- [Searching archived Connection Data](#)

6.19.1 Resynchronization of the Presence Access Privileges in a networked UC Application Environment with several Openfire Servers

If an Openfire server is restored in a networked UC Application environment with several Openfire servers, the presence access privileges of this restored Openfire server must be resynchronized. To do this, all other Openfire servers of the networked UC Application environment must be rebooted independently from each other as soon as restoring the relevant Openfire server is complete and its services have been completely started.

When rebooting the Openfire server make sure not to reboot an Openfire server until the services of the previously started Openfire server have all been booted.

6.19.2 Changing the Openfire Server Certificates

The Openfire server requires appropriate security certificates for encrypted communication. Therefore, the Openfire server keystore contains already pre-

installed, self-signed default certificates. If required, you can replace them, thus adjusting them to an individual certificate strategy.

The following requirements apply for replacing the pre-installed default certificates:

- Altogether two new certificates (*.crt) for the Openfire server are available to you; one of them created using RSA - the other one created with the help of the DSA procedure. Except for the cryptographic procedure used and the aliases, the certificate details must be identical.
- The new certificates for the Openfire server must have an entry in the CommonName field of the unique name (Distinguished Name – DN) of the following format:

*.<XMPP domain>

<XMPP domain> describes the name of the domain the Openfire server manages.

Example: *.openfire_dom01

NOTICE: According to the XMPP specification the names of XMPP domains may contain small letters only.

NOTICE: The XMPP domain name specified in the certificate must correspond to the name specified as server name for the Openfire software.

- The new certificates for the Openfire server must have an entry of the following format as subjectAltName extension:

<XMPP domain>

<XMPP domain> describes the name of the domain the Openfire server manages.

Example: openfire_dom01

NOTICE: According to the XMPP specification the names of XMPP domains may contain small letters only.

NOTICE: The XMPP domain name specified in the certificate must correspond to the name specified as server name for the Openfire software.

- The private keys that associate the new certificates of the Openfire server are available to you in text form.
- For the private keys you have the passwords used for creating these keys.
- You have the certificate (*.crt) of the certificate authority that signed the two new certificates for the Openfire server.

Start the configuration

How to replace the default certificate of the Openfire server:

- 1) Open a shell on the computer system of the Openfire server.

- 2) Execute the following command to stop the Openfire server:

```
/etc/init.d/openfire stop
```

- 3) Switch to the directory in which the Java keytool is installed.

[Determining the Keytool Command](#) describes how to determine this directory.

- 4) Execute the following command in one line in the relevant directory to import the certificate of the certificate authority in the Openfire server keystore.

```
keytool -import -alias rootcert -file <file with the  
certificate of the certificate authority> -keystore /opt/openfire/  
resources/security/truststore -storepass changeit
```

- 5) Execute the following command to start the Openfire server:

```
/etc/init.d/openfire start
```

- 6) Store the two new Openfire certificates and the certificate of the certificate authority on the Openfire server computer system in any directory.

- 7) Switch to the relevant directory in the shell.

- 8) Execute the following command in one line to create a certificate chain from the RSA-based certificate of the Openfire server and the certificate of the certificate authority.

```
cat <RSA certificate file of the Openfire server> <certificate file of the  
certificate authority> > rsa_chain.crt
```

Example: cat rsa_openfire.crt ca_cert.crt > rsa_chain.crt

The certificate chain is stored in the local directory under the name rsa_chain.crt.

- 9) Execute the following command in one line to create a certificate chain from the DSA-based certificate of the Openfire server and the certificate of the certificate authority.

```
cat <DSA certificate file of the Openfire server> <certificate file of the  
certificate authority> > dsa_chain.crt
```

Example: cat dsa_openfire.crt ca_cert.crt > dsa_chain.crt

The certificate chain is stored in the local directory under the name dsa_chain.crt.

- 10) Open a browser and enter the following address to access the administration interface of the Openfire server.

```
https://<IP address of the Openfire server>:9091
```

- 11) Switch on the administration interface to:

Server > TLS / SSL Certificates

- 12) under Server Federation Stores and then under Identity store click on the link Manage Store Contents
- 13) delete the self signed certificates with the delete icon in the delete column
- 14) In the text above Identity you see a link: imported here. Click this link to import certificates. Menu for import opens, enter pass phrase etc.
- 15) click on TLS / SSL Certificates again.
- 16) under XMPP Client Stores and then under Identity store click on the link Manage Store Contents.
- 17) delete the self signed certificates with the delete icon in the delete column
- 18) In the text above Identity you see a link: imported here. Click this link to import certificates. Menu for import opens, enter pass phrase etc.

- 19) Execute the following command in a shell on the computer system of the Openfire server to restart the Openfire server:

```
/etc/init.d/openfire restart
```

You have now replaced the default certificates of the Openfire server.

6.19.3 Searching archived Connection Data

If archiving the instant messaging communication is active in the Openfire server, you can search the communication data collected in this way by individual criteria.

NOTICE: Every 15 minutes, the Openfire system creates automatically a new search index for the archived communication data. Consequently, freshly archived communication data can only be found after the passing of this 15-minute period.

Start the configuration

How to search the archived communication data:

- 1) Log on to the Openfire server under an administrator account.

In doing so please note:

- After a new installation of the Openfire server, the following default password is valid for the user accounts **administrator** and **admin**: **Asd123!**.
- After an upgrade, the following default passwords are valid:
 - For the user account **administrator**, the default password is: **8ABWnmppzEOuxu1q**
 - For the user account **admin**, the default password is: **01*Test!**

NOTICE: The valid passwords can be changed individually on the Openfire administration interface. You find details about this in the Openfire server product documentation.

The Openfire administration interface opens.

- 2) Switch to the **Server > Archiving** tab and select the **Search Archive** menu option.

3) Specify the desired search criteria under:

- **Participant**
- **Date Range**
- **Keywords**

For the search text under **Keywords** applies:

- No case sensitivity.
- Whole words that do not exceed the search text are searched for only. *Example:* The search text **black** will find the words **Black** and **black** in the communication data; but not for example the word **Blackfoot**.
- You can use the wildcard * for any number of characters. *Example:* The search text **black*** will also find for example the word **Blackfoot** in the communication data.

4) Select the **Search** to start searching.

Under **Search Results** you see the communication data that comply with the search criteria.

6.20 Managing the E-Mail Service

This chapter provides information about the following topics:

- [Concept of the E-Mail Service](#)
- [Configuring Send Settings for Notification E-mails](#)
- [Configuring a Callback from a Notification](#)

6.20.1 Concept of the E-Mail Service

OpenScape users can be informed about missed calls by e-mail notification. These notifications are sent by the OpenScape UC Application e-mail service.

You configure settings for sending e-mail notifications (send settings) in the following configuration file:

JMailService.cfg

You find this configuration file after the OpenScape UC Application setup in the following folder of the application computer:

<Osc-Install⁴⁰>/HiPathCA/config/services/default/JMailService/

Please refer to [Send Settings of the E-Mail Service](#) on page 510 see which send settings you can configure in these configuration files.

The subject and body of the e-mail notifications are defined in the file mailPageUC.html. You find this file after the OpenScape UC Application setup in the following folder of the application computer:

<Wc-Install⁴¹>/config/services/default/JMailService/

⁴⁰ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

⁴¹ <Wc-Install> is the web server setup directory: /opt/siemens/HiPathCA or /enterprise/HiPathCA

Send Settings of the E-Mail Service

You can configure the following general settings for sending e-mail notifications with the e-mail service.

- Mail.X-MailerHeader

Possible values:	<Text>
Default setting:	<?x \$TelasWebName ?> journal service
Example:	Call-notification service

Specifies a text that is sent as e-mail header with the e-mail. With the help of this text a user can identify the originator of the e-mail.

- Mail.Charset

Possible values:	
Default setting:	iso-8859-1

Specifies the font in which the e-mail notifications are coded.

- Mail.Server

Possible values:	<Fully qualified name of the SMTP server>
Default setting:	mail.org.de
Example:	Mail.MyCompany.de

Specifies the fully qualified name of the SMTP server via which the e-mail notifications are sent.

- Mail.Sender

Possible values:	<E-mail address>@<Mail.MyCompany.xxx>
Example:	Mail.Sender = Administrator@Unify.de Mail.Sender = Supervisor@Unify.com Mail.Sender = Administrator@Unify.net

Specifies the fully qualified e-mail address inclusive address description used as originator address for sending the e-mail notifications.

NOTICE: The e-mail address used must be configured on the SMTP server used.

- Mail.AuthUser

Possible values:	<User ID>
Default setting:	—

To send e-mails, the e-mail service may have to authenticate at the SMTP server used. [Mail.AuthUser](#) must in this case specify a user account that has the appropriate privileges.

- **Mail.AuthPW**

Possible values:	<User password >
Default setting:	–

Specifies the password that may be used for the authentication with the user account from [Mail.AuthUser](#).

- **Mail.Server.KeepConnection**

Possible values:	– true – Connection stays open. – false – Connection is opened / closed.
Default setting:	true

Specifies whether the e-mail service opens and closes the connection to the SMTP server for each e-mail notification or whether this connection is kept open permanently.

- **ServiceName**

Default setting:	<?x \$TelasWebName ?> Mail Service
Important:	This setting must not be modified!

6.20.2 Configuring Send Settings for Notification E-mails

So that OpenScape users can be informed about missed calls by e-mail notification, you need to configure the send settings of the e-mail service.

Start the configuration

How to configure the send settings of the e-mail service:

- 1) Open the following configuration file with a text editor:

`JMailService.cfg`

You find this file in the following folder of the application computer:

<Osc-Install⁴²>/HiPathCA/config/services/default/JMailService/

- 2) Enter a short, descriptive text in the configuration file under **Mail.X-MailerHeader**.

The e-mail service sends this text in the e-mail header of the notifications. From this header the message recipient should gather that the e-mail is a notification about a missed call.

Example: Notification service

- 3) Verify that the ISO font *iso-8859-1* supports all characters of your national language. If it does not, specify under **Mail.Charset** a font that complies with this requirement.

⁴² <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

- 4) Specify under **Mail.Server** the fully qualified name of the SMTP server. The e-mail service sends the notifications via this SMTP server.

NOTICE: JMailRes_xx.properties can be customized by any administrator and thus it is not included in the update files during a HotFix update. The latest variables can be found in the JMailRes_xx-orig.properties.

- 5) If the e-mail service needs to authenticate at the SMTP server for sending e-mails, execute the following steps.
 - a) Specify under **Mail.AuthUser** a user account that has all privileges for sending e-mails via the relevant SMTP server.
 - b) Specify under **Mail.AuthPW** the password for the specified user account.
- 6) If the e-mail service is to open and close the connection to the SMTP server for each notification, specify value **false** under **Mail.Server.KeepConnection**.
- 7) Save the changes in the configuration file.

You have now configured the send settings of the e-mail service and OpenScape users are informed about missed calls by e-mail notification.

6.20.3 Configuring Settings for Conference Notification

Starting with V11R5.3, a new e-mail notification for conferences is available. It includes HTML format and can be enabled via **JMailService.cfg**.

NOTICE: The **JMailService.cfg** file is located in the following path: /opt/siemens/HiPathCA/config/services/default/JMailService/JMailService.cfg

Follow the steps below to enable the conference notification:

- 1) Open the following configuration file with a text editor: **JMailService.cfg**

You can find this file in the following folder of the application computer:

```
/opt/siemens/HiPathCA/config/services/default/  
JMailService/JMailService.cfg
```

- 2) Set the value of the **Mail.Connection.UseTLS** property to **true** to enable this feature.

```
Mail.Connection.UseTLS = true
```

This property defines whether TLS should be used for the connection to the SMTP server.

If SSL is used, the following procedure must be also followed for the conference notification to work properly:

- 3) Export the SMTP server certificate (e.g. exchange2004.crt).
- 4) Execute the following command:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -  
import -alias smtp_cert -keystore /opt/siemens/share/  
ibm-java-x86_64-80/jre/lib/security/cacerts -file /tmp/  
exchange2004.crt -storepass changeit
```

- 5) Navigate to the `/opt/siemens/share/ibm-java-x86_64-80/jre/lib/security` and execute the following command:

```
/opt/siemens/share/ibm-java-x86_64-80/jre/bin/keytool -
list -keystore cacerts -storepass changeit
```

- 6) Check if the certificate is installed, then restart the symphonia service:

```
/etc/init.d/symphoniad restart
```

6.20.4 Configuring a Callback from a Notification

You can also integrate a callback link in the e-mail notification. This callback link enables a user to initiate a call to the subscriber whose call he/she missed.

Start the configuration

How to configure a callback link for the e-mail notifications:

- 1) Open the following configuration file with a text editor:

```
TelasWeb.cfg
```

You find this file in the following folder of the application computer:

```
<Osc-Install43>/HiPathCA/config/common/
```

- 2) Look for the following entry in the `TelasWeb.cfg` file:

```
<?x set UserEntryURL = "https://<?x $PUBLIC_HOST_NAME ?>:<?
x $SPW_HTTPS1_PORT ?>" ?>
```

- 3) In this entry, replace the expression `<?x $PUBLIC_HOST_NAME ?>` in one of the following ways:
 - If you can reach the computer systems of your OpenScape system only via a proxy server, replace `<?x $PUBLIC_HOST_NAME ?>` with the fully qualified domain name of the proxy server.
 - If you can reach the computer systems of your OpenScape system directly, replace `<?x $PUBLIC_HOST_NAME ?>` in one of the following ways:
 - If you operate your OpenScape system with Integrated Deployment, replace `<?x $PUBLIC_HOST_NAME ?>` with the fully qualified domain name of the application computer.
 - If you operate your OpenScape system with a single frontend computer, replace `<?x $PUBLIC_HOST_NAME ?>` with the fully qualified domain name of the front-end computer.
 - If you operate your OpenScape system with several frontend computers, replace `<?x $PUBLIC_HOST_NAME ?>` with the fully qualified domain name of the load balancer computer used.

⁴³ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 4) If no SSL is to be used for the return call, execute the following steps:
 - a) Look for the following entry in the `TelasWeb.cfg` file:

```
<?x set UserEntryURL = "https://<?x $PUBLIC_HOST_NAME ?>:<?x $SPW_HTTPS1_PORT ?>"
```
 - b) Remove the **S** from the following positions:

```
<?x set UserEntryURL = "http://<?x $PUBLIC_HOST_NAME ?>:<?x $SPW_HTTP1_PORT ?>"
```
- 5) Save the changes in the configuration file.
- 6) Execute one of the following commands on the application computer of OpenScape UC Application to reboot the web server component for the new settings to take effect.
 - **For deployment scenarios with several UC Application computer systems:**

```
/etc/init.d/symphoniad restart WebClient_BE
```
 - **For all other deployment scenarios:**

```
/etc/init.d/symphoniad restart WebClient
```

With this, users can initiate a call from their e-mail notifications.

6.21 Configuring SSO (Single Sign-On)

This chapter provides information about the following topics:

- [Single Sign-on Concept](#)
- **For OpenScape Web Client:**
 - [Configuring the Server for Single Sign-On of the non-SOAP-based Clients](#)
- **For Fusion clients such e. g. OpenScape Fusion for Office:**
 - [Configuring the Server for Single Sign-On of the SOAP-based Clients](#)
- [Deleting Windows Login Information](#)
- [Configuring a Browser for Single Sign-On](#)
- [Configuring UC Application Clients for Single Sign-On](#)
- [Setting up SSO with Windows AD](#)
- [Support of Single Sign On \(SSO\) for multiple Domains](#)

6.21.1 Single Sign-on Concept

Once a Windows user has authenticated at his/her workstation, Single Sign-On enables him/her to deploy further network services without having to authenticate again. The services may be provided by any application servers – in the scope of OpenScape UC Application by the UC Application computer system.

Using Single Sign-On requires the following:

- The user deploys a UC Application client that supports the Single Sign-On feature. Please refer to the *OpenScape UC Application, Client Applications* manual to see which clients have this capability.

- A user account has been configured for the Windows user in the Active Directory of his/her domain controller.

NOTICE: The operating system under which the Active Directory used runs is irrelevant for the Single Sign-On feature of OpenScape UC Application. The only requirement is that the operating system support the Kerberos authentication protocol, AES-256 encryption, and asymmetric encryption. These capabilities have been available since Windows Server 2000.

NOTICE: Starting with UC V11R5 FR9, the Java runtime environment has been updated. Single Sign-On configuration requires **Kerberos AES 256 bits encryption**. Legacy encryption methods (such as RC4 and DES) are no longer supported.

- A technical user account has been configured for the UC Application computer system in the Active Directory of the domain controller.
- A trusted relation has been configured for the UC Application computer system on the domain controller. This requires the application computer of OpenScape UC Application to have a computer account in the relevant Windows domain. You can configure such a computer account by adding the application computer on the relevant domain controller with the administration tool *Active Directory Users and Computers* under **Computers**.
- The browser needs access to the user's authentication information.

IMPORTANT: This is needed also for users which are not SSO enabled!

That's only allowed from Windows when the page (e.g. WebClient) is added to the "Intranet" Security zone.

In order to do so, via **Internet options** (either from control panel -> Network and Internet or from Internet explorer -> options) and follow the following steps

click on **Security** tab

click on **Local intranet**

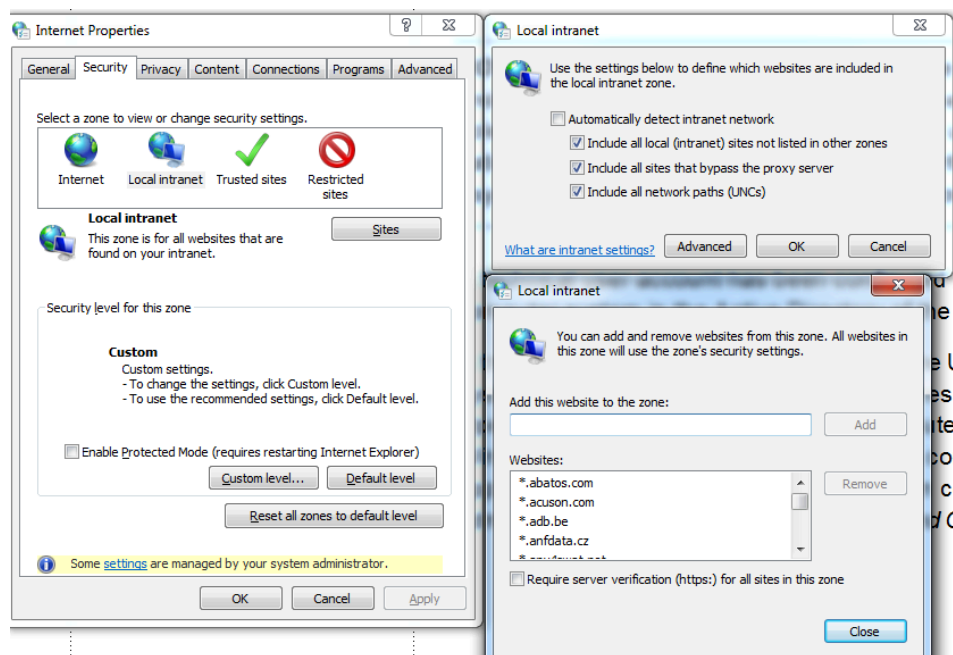
click on **Sites**

click on **Advanced**

specify the server/website (under Add this website to the zone)

click on **Add**

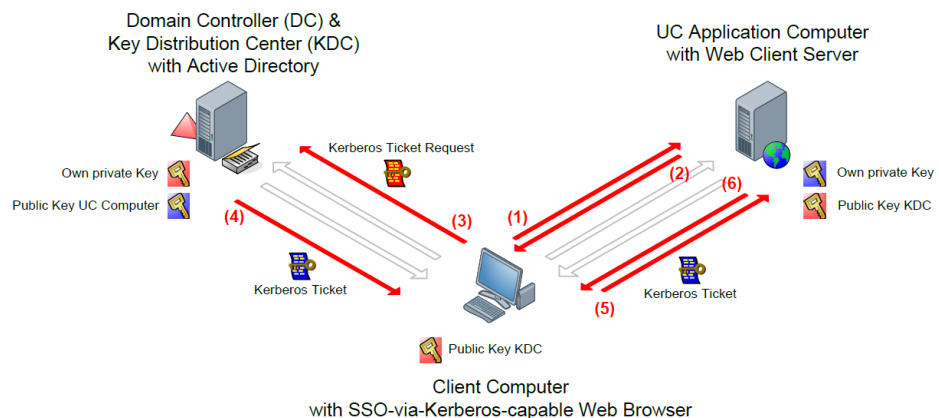
System management for the components of OpenScope UC Application



Single Sign-On of OpenScope UC Application is based on:

- The authentication protocol Kerberos
- The encryption algorithm **AES 256 bits**
- Asymmetric encryption

The following figure shows the collaboration of Single Sign-On components for the OpenScope Web Client.



After the user has logged in at the Windows operating system of a client computer system, the involved components execute the following steps when the user invokes the Web Client service of OpenScope UC Application:

- 1) The web browser of the client computer system requests a web site from the Web Client server of the UC Application computer system.
- 2) The Web Client server responds with the error message that access is denied owing to a missing authentication.
- 3) The client computer system contacts the Key Distribution Center of the relevant domain controller and demands a Kerberos ticket for the UC Application computer system.

The client computer system encrypts this ticket request, so that only the Key Distribution Center can decrypt it. The Key Distribution Center has previously

transferred the public key required for encryption to the client computer system.

- 4) The Key Distribution Center sends a Kerberos ticket to the client computer system.

The Key Distribution Center encrypts this Kerberos ticket so that only the UC Application computer system can decrypt it. The Key Distribution Center has derived the public key required for encryption from the Windows password of a technical user account that has been configured in the Active Directory for the UC Application computer system.

- 5) The web browser forwards the received Kerberos ticket to the UC Application computer system.
- 6) The UC Application computer system decrypts the Kerberos ticket.

The Key Distribution Center has also derived the private key required for this purpose from the Windows password of the technical user account and copied to the UC Application computer system in the scope of the configured trusted relation.

If the log-in module of the UC Application computer system recognizes a valid Kerberos ticket, the Web Client server of the UC Application computer system transfers the requested web site to the web browser of the client computer system without displaying the log-in dialog.

6.21.2 Configuring the Server for Single Sign-On of the non-SOAP-based Clients

NOTICE: You need to execute the configuration steps of this section only if you wish to use the Single Sign-On feature for OpenScape Web Client.

How to configure Single Sign-On of the non-SOAP-based UC Application clients:

- 1) [Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems](#)
- 2) [Configuring a technical User Account](#)
- 3) [Creating the KEYTAB File](#)
- 4) [Configuring JAAS](#)
- 5) [Creating User Assignments](#)
- 6) [Importing User Assignments](#)
- 7) [Restarting OpenScape UC Application](#)

These steps are described in detail in the following sections.

IMPORTANT: Some of the described steps depend on whether you configure Single Sign-On **AES-**, **DES-** or **RC4-based**.

6.21.2.1 Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems

NOTICE: You need to execute the configuration steps of this section only if you wish to use the Single Sign-On feature DES-based.

For Single Sign-On based on DES to run smoothly, DES encryption must be active on all involved client and server computer systems. DES encryption is, however, inactive by default for the following computer systems:

- Computer systems based on Windows 7
- Computer systems based on Windows Server 2008 R2
- Domain controllers based on Windows Server 2008 R2

How to activate DES encryption for these systems:

- 1) Switch to the following location in the Group Policy Management Console (GPMC):

Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

- 2) Select the policy **Network security: Configure encryption types allowed for Kerberos**.
- 3) Select the check boxes of all associated options.
- 4) Click on **OK** to save the modifications.

6.21.2.2 Configuring a technical User Account

Communication between Key Distribution Center and the UC Application computer system is encrypted asymmetrically. The Key Distribution Center derives the keys required for this purpose from the Windows password of a technical user account. This technical user account for the UC Application computer system must be created in the Active Directory.

How to create a user account in the Active Directory is described in the producer documentation of the Active Directory version used.

When creating the technical user account please note the following points depending on whether you wish to use **AES**, **DES** or **RC4**.

- **AES-based Single Sign-On**
 - Activate the **Password never expires** account option.
 - Deactivate the account option **Use Kerberos DES encryption types for this account**.
 - Activate the account option **This Account supports Kerberos AES 256 bits encryption**.
 - Disable the account option **This Account supports Kerberos AES 128 bits encryption**.
- **DES-based Single Sign-On**
 - Activate the **Password never expires** account option.
 - Activate the account option **Use DES encryption types for this account**.

- **RC4-based Single Sign-On**
 - Activate the **Password never expires** account option.
 - Deactivate the account option **Use Kerberos DES encryption types for this account**.
 - Deactivate all account options of the format **This Account supports Kerberos AES xxx bits encryption**.

6.21.2.3 Creating the KEYTAB File

IMPORTANT: The Key Distribution Center authenticates all users / servers that can produce the key from the KEYTAB file. Therefore, the KEYTAB file must be created on a secure computer system, transmitted via a secure path and stored securely.

The KEYTAB file contains Kerberos information that a computer system and its network services can use to uniquely identify against the Key Distribution Center.

Among this KEYTAB file information you find:

- Service principal name⁴⁴ (SPN) of a computer system and its network services
- Private keys for each service principal

The KEYTAB file is created with the Windows support tool `kt pass`. This tool can assign a service principal name to a Windows user account and export the associated private key along with the service principal name to a KEYTAB file.

You find the `kt pass` tool on the setup data carrier of the Windows server operating system.

How to create the KEYTAB file:

- 1) Execute one of the following steps depending on whether you wish to use **AES, DES** or **RC4**.

NOTICE: Please heed case sensitivity for the value of the **-princ** parameter. – Use only capital letters for the domain

⁴⁴ The service principal name is used in the scope of Kerberos for uniquely naming a network service.

name. – The correct writing of the host name is determined by the associated DNS entry.

- **AES-based Single Sign-On**

Execute the following command in one line in a domain controller command line to create the KEYTAB file:

```
ktpass -princ HTTP/<FQDN45>@<domain46> -mapuser <Netbios domain47>\<Name of the techn. user account>  
-pass <Password for the techn. user account>  
-out krb5.keytab  
-crypto AES256-SHA1  
-ptype KRB5_NT_PRINCIPAL
```

Example:

```
ktpass -princ HTTP/oscservers.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+  
-out krb5.keytab  
-crypto AES256-SHA1
```

⁴⁵ Use the FQDN of one of the following computer systems on the basis of the actual host name and not based on the alias name: – For deployment scenarios without individual front-end computer: FQDN of the application computer – For deployment scenarios with exactly one individual front-end computer: FQDN of the front-end computer – For deployment scenarios with several individual front-end computers: FQDN of the associated load balancer

⁴⁶ Use the name of the domain the Windows users to be registered are assigned to.

⁴⁷ Pre-Windows 2000 domain name

-ptype KRB5_NT_PRINCIPAL

- **DES-based Single Sign-On**

Execute the following command in one line in a command line of the domain controller to create the KEYTAB file:

NOTICE: The **-TrustEncryp DES** parameter is available for Windows Server 2003 R2 only.

```
ktpass -princ HTTP/<FQDN48>@<domain49> -mapuser <Netbios  
domain50>\<name of the techn. user account >  
-pass <password for the techn. user account >  
-out krb5.keytab  
-crypto des-cbc-md5  
-ptype KRB5_NT_PRINCIPAL  
+DesOnly  
-TrustEncryp DES
```

Example:

```
ktpass -princ HTTP/oscservers.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+  
-out krb5.keytab  
-crypto des-cbc-md5  
-ptype KRB5_NT_PRINCIPAL +DesOnly
```

⁴⁸ Use the FQDN of one of the following computer systems on the basis of the actual host name and not based on the alias name: – For deployment scenarios without individual front-end computer: FQDN of the application computer – For deployment scenarios with exactly one individual front-end computer: FQDN of the front-end computer – For deployment scenarios with several individual front-end computers: FQDN of the associated load balancer

⁴⁹ Use the name of the domain the Windows users to be registered are assigned to.

⁵⁰ Pre-Windows 2000 domain name

-TrustEncryp DES

- **RC4-based Single Sign-On** Execute the following command in one line in a command line of the domain controller to create the KEYTAB file:

```
ktpass -princ HTTP/<FQDN51>@<domain52> -mapuser <Netbios domain53>\<name of the techn. user account >  
-pass <password for the techn. user account >  
-out krb5.keytab  
-crypto rc4-hmac-nt  
-ptype KRB5_NT_PRINCIPAL
```

Example:

```
ktpass -princ HTTP/oscservice.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+  
-out krb5.keytab  
-crypto rc4-hmac-nt  
-ptype KRB5_NT_PRINCIPAL
```

- 2) To check the new SPN user account assignment, execute the following command in one line in the command line of the domain controller:

```
setspn -L <Name of the technical user account >
```

Example:

```
setspn -L ssoadmin
```

The output may display only one single entry for the service principal name used for creating the KEYTAB file.

IMPORTANT: A service principal name must not be assigned to several user accounts at the same time. If the setspn -L example output shows a multiple assignment just the same, you must delete all excess assignments with the following command: setspn -D HTTP/<DP name> <account name> *Example:* setspn -D HTTP/oscservice.net techuser Always specify the service principal name for <DP name> in the deletion command as it was shown in the setspn -L example output.

⁵¹ Use the FQDN of one of the following computer systems on the basis of the actual host name and not based on the alias name: – For deployment scenarios without individual front-end computer: FQDN of the application computer – For deployment scenarios with exactly one individual front-end computer: FQDN of the front-end computer – For deployment scenarios with several individual front-end computers: FQDN of the associated load balancer

⁵² Use the name of the domain the Windows users to be registered are assigned to.

⁵³ Pre-Windows 2000 domain name

- 3) Copy the KEYTAB file `krb5.keytab` to the following location:
 - For Integrated Deployment:
To the `/enterprise` directory of the application computer (active and, if required, passive)
 - For Small Deployment:
To the `/opt/siemens` directory of the application computer (active and, if required, passive)
 - For all other deployment scenarios:
To the `/opt/siemens` directory of the front-end computers
- 4) Switch to the directory in which you have stored the KEYTAB file.
- 5) Execute the following command to assign the KEYTAB file to user **sym** and group **sym**:

```
chown sym:sym krb5.keytab
```

You have now created the KEYTAB file for the non-SOAP-based clients.

IMPORTANT: The KEYTAB file `krb5.keytab` in the `/opt/siemens` directory of a UC Application computer system is not automatically backed up when you perform a backup via the CMP. Therefore, you must back up the relevant KEYTAB file manually lest it gets lost during a system restore. After the restore you must copy the KEYTAB file in the correct directory also manually.

NOTICE: This KEYTAB file concerns the communication of the non-SOAP-based clients with the UC Application front-end services via the ports 8443 (HTTPS) and 7789 (HTTP).

6.21.2.4 Configuring JAAS

OpenScape UC Application uses the authentication and authorization service JAAS for the Kerberos authentication. JAAS must therefore be configured for the OpenScape UC Application application computer.

JAAS is configured via the following configuration files.

- `Krb5.conf`
- `jaas.cfg`
- `authentication.cfg`

How to configure JAAS:

- 1) Open the following configuration file with a text editor:

`Krb5.conf`

You find this file in the following folder of the application computer:

`<Osc-Install54>/common/conf/`

⁵⁴ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 2) Execute one of the following steps depending on whether you wish to use **AES, DES** or **RC4**.
 - **DES-based Single Sign-On**

Specify the name you wish to assign to the Kerberos Realm for the **default_realm** parameter in the **[libdefaults]** section.

In doing so, use capital letters only.

For example, you can enter the name of the Windows domain in capital letters.
 - **AES- or RC4-based Single Sign-On**

Change the **KERBEROS_DOMAIN.NET** entry in the **[realms]** section to the name you wish to assign to the Kerberos realm. In doing so, use capital letters only.

For example, you can enter the name of the Windows domain in capital letters.
- 3) **DES-based Single Sign-On only** Change the **EXAMPLE.NET** entry in the **[realms]** section to the Kerberos Realm you specified for the **default_realm** parameter.
- 4) Specify the IP address of the relevant Windows domain controller for the **kdc** parameter under the Kerberos realm in the **[realms]** section. Keep port number **88**.

NOTICE: If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

- 5) Execute one of the following steps depending on whether you wish to use **AES, DES** or **RC4**.
 - **DES-based Single Sign-On**

In the **[domain_realm]** section, assign the Windows domain to the Kerberos realm. Use the correct upper and lower case writing for the name of the Windows domain; for the Kerberos realm name use capital letters only.

```
[libdefaults]
default_realm = <Kerberos-Realm>
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5
default_checksum = rsa-md5
kdc_timesync = 0

[realms]
<Kerberos realm>= {
kdc = <IP / FQDN of the Windows domain controller>:88
}
[domain_realm] .
<name of the Windows domain> = <Kerberos realm>

[logging]
default = krb5.log
```

Example:


```
[libdefaults]
default_realm = COMPANY.COM
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5
default_checksum = rsa-md5
kdc_timesync = 0

[realms]
COMPANY.COM
kdc = dc.company.com :88
}
[domain_realm]
.company.com = COMPANY.COM
[logging]
default = krb5.log
```

NOTICE: Windows supports under [realms] a single entry only. Environments that require a second realms entry are not supported on the operating system side.

- **AES- or RC4-based Single Sign-On**

In the [domain_realm] section, assign the Windows domain to the Kerberos realm. Use the correct upper and lower case writing for the name of the Windows domain; for the Kerberos realm name use capital letters only.

```
[libdefaults]
kdc_timesync = 0
[realms]
<Kerberos realm> = {
kdc = <IP/FQDN of the Windows domain controller>:88
}
[domain_realm]
.<name of the Windows domain> = <Kerberos realm>
```

Example:

```
[libdefaults]
kdc_timesync = 0
[realms]
COMPANY.COM = { kdc = dc.company.com:88
}
[domain_realm]
.company.com = COMPANY.COM
```

NOTICE: Windows supports under [realms] a single entry only. Environments that require a second realms entry are not supported on the operating system side.

- 6) Save the changes in the Krb5.conf file.

- 7) Open the following configuration file with a text editor:

jaas.cfg

You find this file in the following folder of the application computer:

<Osc-Install⁵⁵>/HiPathCA/config/common/

- 8) Attach the following to the end of the configuration file:

```
SSOLogin
{com.siemens.ca.security.auth.winsso.SPNEGOKrbLogin
  required
  useSharedState=false
  converterClass="com.siemens.ca.security.auth.UidResolver"
  EXTERNAL_SYSTEM_NAME= < individual expression >
  uidToLowerCase=false
  principal=" < service principal name > ";
};
com.ibm.security.jgss.initiate
{
  com.ibm.security.auth.module.Krb5LoginModule required;
};
com.ibm.security.jgss.accept
{
  com.ibm.security.auth.module.Krb5LoginModule required
  debug=false
  credsType=acceptor

  useKeytab= " <path to keytab file> "
  principal=" < service principal name > ";
};
```

- 9) Specify an individual expression for the **EXTERNAL_SYSTEM_NAME** parameter without quotation marks.

IMPORTANT: The expression used must not contain any blanks.

Example: WindowsSSO

You will later use this identifier to assign the SSO login to OpenScape users.

- 10) Specify the service principal name for the two **principal** parameters that you also used in the KEYTAB file (cf. [Creating the KEYTAB File](#) on page 519).

Please heed case sensitivity.

Example:

```
SSOLogin
{
  com.siemens.ca.security.auth.winsso.SPNEGOKrbLogin
    required
  useSharedState=false
```

⁵⁵ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

```
converterClass="com.siemens.ca.security.auth.UidResolver"
EXTERNAL_SYSTEM_NAME= WindowsSSO
uidToLowerCase=false
principal=" HTTP/oscserver.net@COMPANY.COM ";
};
com.ibm.security.jgss.initiate
{
com.ibm.security.auth.module.Krb5LoginModule required;
};
com.ibm.security.jgss.accept
{
com.ibm.security.auth.module.Krb5LoginModule required
debug=false
credsType=acceptor
useKeytab="/opt/siemens/krb5.keytab"
principal=" HTTP/oscserver.net@COMPANY.COM ";
};
```

11) Save the changes in the file `jaas.cfg`.

12) Open the following configuration file with a text editor:

`authentication.cfg`

You find this file in the following folder of the application computer:

`<Osc-Install56>/HiPathCA/config/common/`

13) Specify value **SSOLogin** for the **com.siemens.ca.server.config.jaas.appName** parameter.

You have now configured JAAS.

6.21.2.5 Creating User Assignments

For Single Sign-On to run smoothly, you need to assign the name of the respectively associated Windows user account to the relevant OpenScape user accounts. Import the corresponding user assignments in OpenScape UC Application for this purpose.

Before you can import the user assignments in OpenScape UC Application you need to create the relevant assignments.

How to create the user assignments:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.

The dialog for exporting configurations opens.

⁵⁶ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.
- 8) Open the downloaded Zip file and open the following Zip file contained therein:

Package_domainmanagement_domainmanagement001.zip

- 9) In there open the following file with a text editor:

domain_configuration.csv

NOTICE: You should use the text editor Notepad++. If you use other text editors you need to make sure that no Byte-Order-Mark – BOM is used.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the user assignments under the entry that begins with `##ExternalId`.
 - The fields of an entry are separated from each other by semicolon.
- 10) Look for the user assignments section in the file. This section begins with the following line:

`##ExternalId;externalId;...`

- 11) Remove all lines that do not belong to the user assignments section from the file.

In a file without existing user assignment, only the following line then remains:

`##ExternalId;externalId;...`

- 12) Add to the file under `##ExternalId` all required user assignments that assign the respectively associated Microsoft Exchange user account to the relevant OpenScope user accounts.

In doing so please heed the following:

- The following data special characters must be marked by the escape character `\` for later import: `, \ # =`
- Create a new `ExternalId` entry for each assignment.
- Enter the reserved name **ExternalId** under **##ExternalId**.

This name defines the entry as user assignment.

- Enter the Windows login ID of the relevant OpenScope user account under **externalId**. In doing so, use the `@`-notation and heed case sensitivity.

Use only capital letters for the domain name.

Example: `mSample@COMPANY.COM`

- Always specify the **false** value under **isContactMaster**.
- Always specify the **false** value under **isProvisioningMaster**.
- Specify under **assignedExternalSystemId** the expression that you previously defined in the `jaas.cfg` file for the **EXTERNAL_SYSTEM_NAME** parameter.

Example: `WindowsSSO`

- Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: `mSample@system`

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

<code>##ExternalId</code>	<code>externalId</code>	<code>assignedUserIdentity</code>
<code>ExternalId</code>	<code>mSample@COMPANY.COM</code>	<code>mSample@system</code>
<code>ExternalId</code>	<code>tBrown@COMPANY.COM</code>	<code>tBrown@system</code>
...	...	...

<code>assignedExternalSystemId</code>	<code>isContactMaster</code>	<code>isProvisioningMaster</code>	...
<code>WindowsSSO</code>	<code>false</code>	<code>false</code>	...
<code>WindowsSSO</code>	<code>false</code>	<code>false</code>	...
...	...	...	...

```
##ExternalId;externalId;assignedUserIdentity;
assignedExternalSystemId;isContactMaster;
isProvisioningMaster;additionalInfo
```

```
ExternalId;mSample@COMPANY.COM;mSample@system;  
WindowsSSO;false;false;  
  
ExternalId;tBrown@COMPANY.COM;tBrown@system;  
WindowsSSO;false;false;  
...
```

- 13) Save the supplemented file under the name `domain_configuration.csv` in CSV format.
- 14) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

You have now created the required user assignments.

6.21.2.6 Importing User Assignments

You need to import the user assignments just created in OpenScape UC Application.

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.
The dialog for importing a configuration opens.
- 4) In the **Import file** field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file.
- 5) Click on **Next**.
- 6) Check that the **Common Management Platform** option has been selected under **Type of file to be imported**.
- 7) Check that the **Domain Management** option has been selected under **Included type of data**.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

You have now imported the user assignments in OpenScape UC Application.

6.21.2.7 Restarting OpenScape UC Application

You need to reboot OpenScape UC Application for the Single Sign-On settings to take effect.

Reboot OpenScape UC Application by executing the following commands:

```
/etc/init.d/symphoniad stop  
/etc/init.d/symphoniad start
```

All Single Sign-On settings are now effective.

NOTICE: No restart of the OpenScape UC Application is needed if only the user externalID is modified.

6.21.3 Configuring the Server for Single Sign-On of the SOAP-based Clients

NOTICE: If Single Sign-On has already been configured for a UC Application user to deploy the CMP, this user cannot additionally deploy Single Sign-On by means of SOAP-based UC Application clients.

How to configure Single Sign-On of the SOAP-based UC Application clients:

- 1) [Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems](#)
- 2) [Configuring a technical User Account](#)
- 3) [Creating the KEYTAB File](#)
- 4) [Configuring the SPNEGO-IAE Service](#)
- 5) [Configuring JAAS_IBM](#)
- 6) [Creating and importing User Assignments](#)
- 7) [Restarting OpenScape UC Application](#)

These steps are described in detail in the following sections.

IMPORTANT: Some of the described steps depend on whether you configure Single Sign-On **AES-**, **DES-** or **RC4-based**.

6.21.3.1 Preliminaries for Windows 7 and Windows Server 2008 R2 Operating Systems

NOTICE: You need to execute the configuration steps of this section only if you wish to use the Single Sign-On feature DES-based.

NOTICE: You may have already executed the configuration steps of this section for Single Sign-On of non-SOAP-based UC Application clients. In this case please check the described settings once again.

For Single Sign-On based on DES to run smoothly, DES encryption must be active on all involved client and server computer systems. DES encryption is, however, inactive by default for the following computer systems:

- Computer systems based on Windows 7
- Computer systems based on Windows Server 2008 R2
- Domain controllers based on Windows Server 2008 R2

How to activate DES encryption for these systems:

- 1) Switch to the following location in the Group Policy Management Console (GPMC):
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
- 2) Select the policy **Network security: Configure encryption types allowed for Kerberos**.
- 3) Select the check boxes of all associated options.
- 4) Click on **OK** to save the modifications.

6.21.3.2 Configuring a technical User Account

NOTICE: You need to execute the configuration steps of this section only if at least one of the following requirements applies:
– You use at least one individual front-end computer. – You use Single Sign-On for SOAP-based UC Application clients only.

Communication between Key Distribution Center and the UC Application computer system is encrypted asymmetrically. The Key Distribution Center derives the keys required for this purpose from the Windows password of a technical user account. This technical user account for the UC Application computer system must be created in the Active Directory.

How to create a user account in the Active Directory is described in the producer documentation of the Active Directory version used.

When creating the technical user account please note the following points depending on whether you wish to use **AES**, **DES** or **RC4**.

- **AES-based Single Sign-On**
 - Activate the **Password never expires** account option.
 - Deactivate the account option **Use Kerberos DES encryption types for this account**.
 - Activate the account option **This Account supports Kerberos AES 256 bits encryption**.
 - Disable the account option **This Account supports Kerberos AES 128 bits encryption**.
- **DES-based Single Sign-On**
 - If you have already created a technical user account for non-SOAP-based UC Application clients, it must have a different name.
 - Activate the **Password never expires** account option.
 - Activate the account option **Use DES encryption types for this account**.
- **RC4-based Single Sign-On**
 - If you have already created a technical user account for non-SOAP-based UC Application clients, it must have a different name.
 - Activate the **Password never expires** account option.
 - Deactivate the account option **Use Kerberos DES encryption types for this account**.
 - Deactivate all account options of the format **This Account supports Kerberos AES xxx bits encryption**.

6.21.3.3 Creating the KEYTAB File

NOTICE: You need to execute the configuration steps of this section only if at least one of the following requirements applies:

- You use at least one individual front-end computer.
- You use Single Sign-On for SOAP-based UC Application clients only.

If you skip the configuration steps of this section, you need to use in the following chapters the KEYTAB file and the service principal name you use for the Single Sign-On of SOAP-based UC Application clients.

NOTICE: The Key Distribution Center authenticates all users / servers that can produce the key from the KEYTAB file. Therefore, the KEYTAB file must be created on a secure computer system, transmitted via a secure path and stored securely.

The KEYTAB file contains Kerberos information that a computer system and its network services can use to uniquely identify against the Key Distribution Center.

Among this KEYTAB file information you find:

- Service principal name⁵⁷ (SPN) of a computer system and its network services
- Private keys for each service principal

The KEYTAB file is created with the Windows support tool `kt pass`. This tool can assign a service principal name to a Windows user account and export the associated private key along with the service principal name to a KEYTAB file.

You find the `kt pass` tool on the setup data carrier of the Windows server operating system.

How to create the KEYTAB file:

⁵⁷ The service principal name is used in the scope of Kerberos for uniquely naming a network service.

- 1) Execute one of the following steps depending on whether you wish to use **AES**, **DES** or **RC4**.

NOTICE: Please heed case sensitivity for the value of the -**princ** parameter.

- Use only capital letters for the domain name.
 - The correct writing of the host name is determined by the associated DNS entry.
-

- **AES-based Single Sign-On**

Execute the following command in one line in a domain controller command line to create the KEYTAB file:

```
ktpass -princ HTTP/<FQDN58>@<domain59>  
-mapuser <Netbios domain60>\<Name of the techn. user account >  
-pass <Password for the techn. user account >  
-out krb5.keytab  
-crypto AES256-SHA1  
-ptype KRB5_NT_PRINCIPAL
```

Example:

```
ktpass -princ HTTP/oscservers.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+  
-out krb5.keytab  
-crypto AES256-SHA1
```

⁵⁸ Use the FQDN of one of the following computer systems on the basis of the actual host name and not based on the alias name: – For deployment scenarios without individual front-end computer: FQDN of the application computer – For deployment scenarios with exactly one individual front-end computer: FQDN of the front-end computer – For deployment scenarios with several individual front-end computers: FQDN of the associated load balancer

⁵⁹ Use the name of the domain the Windows users to be registered are assigned to.

⁶⁰ Pre-Windows 2000 domain name

```
-ptype KRB5_NT_PRINCIPAL
```

- **DES-based Single Sign-On**

Execute the following command in one line in a command line of the domain controller to create the KEYTAB file:

NOTICE: The **-TrustEncryp DES** parameter is available for Windows Server 2003 R2 only.

```
ktpass -princ HTTP/<FQDN61>@<domain62>  
-mapuser <Netbios domain63>\<name of the techn. user account >  
-pass <password for the techn. user account >  
-out krb5.keytab  
-crypto des-cbc-md5  
-ptype KRB5_NT_PRINCIPAL  
+DesOnly  
-TrustEncryp DES
```

Example:

```
ktpass -princ HTTP/oscservice.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+ -out krb5.keytab  
-crypto des-cbc-md5  
-ptype KRB5_NT_PRINCIPAL  
+DesOnly
```

⁶¹ Always use the FQDN of the application computer on the basis of the actual host name and not based on the alias name.

⁶² Use the name of the domain the Windows users to be registered are assigned to.

⁶³ Pre-Windows 2000 domain name

-TrustEncryp DES

In doing so, use the technical user account you created in [Configuring a technical User Account](#) on page 532.

- **RC4-based Single Sign-On**

Execute the following command in one line in a command line of the domain controller to create the KEYTAB file:

```
ktpass -princ HTTP/<FQDN64>@<domain65> -mapuser <Netbios domain66>\<name of the techn. user account >  
-pass <password for the techn. user account >  
-out krb5.keytab  
-crypto rc4-hmac-nt  
-ptype KRB5_NT_PRINCIPAL
```

Example:

```
ktpass -princ HTTP/oscservice.net@COMPANY.COM  
-mapuser COMPANY\ssoadmin  
-pass !Osc123+  
-out krb5.keytab  
-crypto rc4-hmac-nt  
-ptype KRB5_NT_PRINCIPAL
```

In doing so, use the technical user account you created in [Configuring a technical User Account](#) on page 532.

- 2) To check the new SPN user account assignment, execute the following command in one line in the command line of the domain controller:

```
setspn -L <Name of the technical user account >
```

Example: setspn -L ssoadmin

The output may display only one single entry for the service principal name used for creating the KEYTAB file.

IMPORTANT: A service principal name must not be assigned to several user accounts at the same time. If the setspn -L example output shows a multiple assignment just the same, you must delete all excess assignments with the following command: setspn -D HTTP/<DP name> <account name> *Example:* setspn -D HTTP/oscservice.net techuser Always specify the service principal name for <DP name> in the deletion command as it was shown in the setspn -L example output.

⁶⁴ Always use the FQDN of the application computer on the basis of the actual host name and not based on the alias name.

⁶⁵ Use the name of the domain the Windows users to be registered are assigned to.

⁶⁶ Pre-Windows 2000 domain name

- 3) Copy the KEYTAB file `krb5.keytab` to the following location:
 - For Integrated Deployment: To the `/enterprise` directory of the application computer (active and, if required, passive)
 - For all other deployment scenarios: To the `/opt/siemens` directory of the application computer (active and, if required, passive)
- 4) Switch to the directory in which you have stored the KEYTAB file.
- 5) Execute the following command to assign the KEYTAB file to user **sym** and group **sym**:

```
chown sym:sym krb5.keytab
```

You have now created the KEYTAB file for the SOAP-based clients.

IMPORTANT: The KEYTAB file `krb5.keytab` in the `/opt/siemens` directory of a UC Application computer system is not automatically backed up when you perform a backup via the CMP. Therefore, you must back up the relevant KEYTAB file manually lest it gets lost during a system restore. After the restore you must copy the KEYTAB file in the correct directory also manually.

NOTICE: This KEYTAB file concerns the communication of the SOAP-based clients with the application computer via the ports 4708 (HTTP) and 4709 (HTTPS).

6.21.3.4 Configuring the SPNEGO-IAE Service

Configure in the configuration file of the SPNEGO-IAE service the SPNEGO-IAE service principal name by executing one of the following commands in a shell on the application computer.

In doing so, replace the expression *<service principal name>* with the service principal name you used for creating the KEYTAB file (cf. e. g. [Creating the KEYTAB File](#) on page 533).

NOTICE: Instead of executing the following sed-commands you can also proceed as described under [Configuration alternative](#).

NOTICE: Please heed case sensitivity for the service principal name.

For Integrated Deployment:

```
sed -i 's#@SPNEGOIAE_SERVICEPRINCIPALNAME@#< service  
principal name> #g' /enterprise/common/conf/config-beans/  
*
```

For all other deployment scenarios:

```
sed -i 's#@SPNEGOIAE_SERVICEPRINCIPALNAME@# < service  
principal name > #g' /opt/siemens/common/conf/config-  
beans/*
```

Example of Integrated Deployment:

```
sed -i 's#@SPNEGOIAE_SERVICEPRINCIPALNAME@#HTTP/  
oscservice.net@COMPANY.COM#g' /enterprise/common/conf/  
config-beans/*
```

You have now configured the SPNEGO-IAE service.

Configuration alternative

If you need to change the just configured SPNEGO-IAE service principal name retrospectively, you cannot use the described sed-command for this purpose anymore. There is an alternative for this case:

- 1) Open a shell on the application computer and switch to the following directory:

```
<Osc-Install67>/common/conf/config-beans
```

- 2) Execute in the directory the following command to find the appropriate configuration file:

```
ls * | grep SPNEGO *
```

The command output in the shell has the format:

```
instance_b036b113-9463-40af-8d48-  
a42182479a9f.xml: <InstanceData  
className="com.siemens.symphonia.spnegoiae.impl.SpnegoIaeImpl"  
displayName="SPNEGO IAE service" enabled="true"  
guid="b036b113-9463-40af-8d48-a42182479a9f"  
version="1.0.0">
```

The name at the beginning of the output specifies the name of the configuration file the contents of which you need to change.

In the above example this would be:

```
instance_b036b113-9463-40af-8d48-a42182479a9f.xml
```

- 3) Open the relevant file with a text editor.
- 4) Configure the desired service principal name for the following parameter:

ServicePrincipalName

```
<Property name="ServicePrincipalName"  
value="HTTP/oscservice.net@COMPANY.COM"/>
```

- 5) Save the changed setting in the configuration file.

6.21.3.5 Changing the Buffer Sizes

To change the buffer sizes, follow the steps below:

⁶⁷ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

- 1) Open the following file with a text editor:

`<Osc-Install68>/common/conf/symom.config.xml`

- 2) Edit the values of the properties `SocketFactory.MinBufferSize` and `SocketFactory.MaxBufferSize` accordingly.

The suggested minimum and maximum buffer size values are the following:

`"SocketFactory.MinBufferSize" value="65536"`

`"SocketFactory.MaxBufferSize" value="1048576"`

For example:

```
<extension
  class="com.siemens.symphonia.remoting.socket.SecureSocketTransportExtensionFactory"
  disabled="false">
<property name="SocketFactory.MinBufferSize" value="65536"/>
<property name="SocketFactory.MaxBufferSize" value="1048576"/>
```

- 3) Save the changes in the file.

6.21.3.6 Configuring JAAS_IBM

OpenScape UC Application uses the authentication and authorization service JAAS for the Kerberos authentication. JAAS must therefore be configured for the OpenScape UC Application application computer.

How to configure JAAS_IBM:

- 1) Open the following configuration file with a text editor:

`krb5-jaas_ibm.conf`

You find this file in the following folder of the application computer:

`<Osc-Install69>/common/conf/`

- 2) Change the path for the KEYTAB file in the **useKeytab** entry.
- 3) Change the setting for **debug** to false.

Example:

```
com.ibm.security.jgss.accept {
  com.ibm.security.auth.module.Krb5LoginModule required
  credsType=acceptor useKeytab=
    "/opt/siemens/krb5.keytab"
  principal="HTTP/oscservers.net@COMPANY.COM";
```

⁶⁸ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

⁶⁹ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- 4) Specify in the **principal** entry the service principal name you defined in the KEYTAB file (cf. e. g. [Creating the KEYTAB File](#) on page 533).

NOTICE: Please heed case sensitivity for the service principal name.

Example:

```
com.ibm.security.jgss.accept {
  com.ibm.security.auth.module.Krb5LoginModule required
  credsType=acceptor
  useKeytab="/opt/siemens/krb5.keytab"
  principal=" HTTP/oscserver.net@COMPANY.COM ";
```

You have now configured JAAS_IBM.

6.21.3.7 Creating and importing User Assignments

Additional user assignments will be required. How to configure them:

- 1) Always create additional user assignments as described in [Creating User Assignments](#) on page 527.

Creating additional user assignments deviates in the following points from the description in [Creating User Assignments](#) on page 527.

- Enter under **externalId** the Windows login ID of the relevant OpenScape user account *without the domain name*.

Example: mSample

- Enter under **assignedExternalSystemId** the *domain name you used for creating the KEYTAB file* (cf. [Creating the KEYTAB File](#) on page 533).

In doing so, use capital letters only.

Example: COMPANY.COM

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	assignedUserIdentity
ExternalId	mSample	mSample@system
ExternalId	tBrown	tBrown@system
...	...	...

assignedExternalSystemId	isContactMaster	isProvisioningMaster	...
COMPANY.COM	false	false	...

assignedExternalSystemId	isContactMaster	isProvisioningMaster	...
COMPANY.COM	false	false	...
...	...	...	...

```
##ExternalId;externalId;assignedUserIdentity;assignedExternalSystemId;isContactMaster;isProvisioningMaster;additionalInfo
```

```
ExternalId;mSample;mSample@system;COMPANY.COM;false;false;
```

```
ExternalId;tBrown;tBrown@system;COMPANY.COM;false;false;
```

```
...
```

- 2) Import the additional user assignments as described in [Importing User Assignments](#) on page 530.

6.21.3.8 Restarting OpenScape UC Application

You need to reboot OpenScape UC Application for the Single Sign-On settings to take effect.

Reboot OpenScape UC Application by executing the following commands:

```
/etc/init.d/symphoniad stop
```

```
/etc/init.d/symphoniad start
```

All Single Sign-On settings are now effective.

6.21.4 Deleting Windows Login Information

To ensure that Single Sign-On works correctly, you must delete already stored Windows login information using the Windows Credential Manager.

You can open the Windows Credential Manager of a Windows computer system via the control panel.

In case of Windows 7, Windows login information already stored is displayed in the Windows Credential Manager under **Windows Credentials** and you can delete it there individually.

6.21.5 Configuring a Browser for Single Sign-On

Depending on the browser used, you need to perform settings in the browser for Single Sign-On.

- [Internet Explorer Settings](#)
- [Firefox Settings](#)

6.21.5.1 Internet Explorer Settings

The following browser settings must be performed for using Single Sign-On in the Internet Explorer.

- The following must be assigned to the **Local Intranet** security zone:
 - For deployment scenarios without individual front-end computer the fully qualified domain name of the application computer.
 - For all other deployment scenarios the fully qualified domain names of the front-end computer systems.

You can achieve this in two ways.

- Add the required domain names in the following place of the browser settings:

Tools > Internet Options > Security > Local intranet > Sites > Advanced

- Add the required computer systems to the Active Directory under **users and computers**.

- The following default browser settings must be active:

- **Enable Integrated Windows Authentication** under

Tools > Internet Options > Advanced > Security

- **Automatic logon only in Intranet zone"** under

Tools > Internet Options > Security > Local Intranet > Security level for this zone > Custom level > User Authentication > Logon

6.21.5.2 Firefox Settings

How to perform internal browser settings for Firefox:

NOTICE: If you have configured the Single Sign-On option for a UC Application system, you must execute the following configuration steps for the Firefox browsers of all associated UC Application users. This includes the Firefox browsers of the UC Application users who do not use Single Sign-On.

- 1) Start the Firefox browser.
- 2) Enter **about:config** in the address field and press the return key.
- 3) Confirm the security prompt.

The page with internal browser settings is displayed.

- 4) Select the name of the following setting with a doubleclick:

`network.automatic-ntlm-auth.trusted-uris`

The dialog for entering a string value opens.

5) Specify the following in the input field:

- For deployment scenarios without individual front-end computer the fully qualified domain name of the application computer.
- For all other deployment scenarios the fully qualified domain names of the front-end computer systems.

Example: oscuc.MyCompany.com

6) Confirm the entry with **OK**.

7) Select the name of the following setting with a doubleclick:

network.negotiate-auth.trusted-uris

The dialog for entering a string value opens.

8) Specify the following in the input field:

- For deployment scenarios without individual front-end computer the fully qualified domain name of the application computer.
- For all other deployment scenarios the fully qualified domain names of the front-end computer systems.

Example: oscuc.MyCompany.com

9) Confirm the entry with **OK**.

You have now configured the internal browser settings for Firefox.

6.21.6 Configuring UC Application Clients for Single Sign-On

The following UC Application clients require special settings for users to deploy Single Sign-On.

- Client applications of type OpenScape Fusion
- OpenScape Conference Extension for Microsoft Outlook (for deployment scenarios with front-end computer)

How to perform such settings is outlined in the associated client manuals.

6.21.7 Setting up SSO with Windows AD

call new script with parameters:

```
configureSSO.sh keytabfile-web keytabfile-soap
externalSystem kdc logindialog
(the script is in directory :
/opt/siemens/servicetools/security/sso/configureSSO.sh )
```

Extract server principal name and realm from keytab file

```
/opt/siemens/share/ibm-java-i386-60/jre/bin/klist -e -K -
k /opt/siemens/krb5.keytab
```

Key table:

```
/opt/siemens/krb5.keytab [1] principal: HTTP/
emma2.helena.gr@HELENA.GR KVNO: 3
```

6.21.7.1 SPNEGO IAE and/or WebClient Configuration File: /opt/siemens/common/conf/krb5.conf

```
# -----
# Kerberos configuration file for running the JGSS
# applications.
# Modify the entries to suit your environment.
# See http://web.mit.edu/kerberos/www/krb5-1.6/krb5-1.6/
# doc/krb5-admin.html#krb5.conf
# -----
[libdefaults]
default_realm = HELENA.GR
default_tkt_enctypes = des-cbc-md5
default_tgs_enctypes = des-cbc-md5
default_checksum = rsa-md5
kdc_timesync = 0

[realms]
HELENA.GR = {
kdc = 10.9.136.56:88
}

[domain_realm]
.helena.gr = HELENA.GR
[logging]
default = krb5.log
```

6.21.7.2 WebClient only Configuration

```
1. File /opt/siemens/HiPathCA/config/common/jaas.cfg
SSOLogin
{
com.siemens.ca.security.auth.winsso.SPNEGOKrbLogin
    required
useSharedState=false
converterClass="com.siemens.ca.security.auth.UidResolver"
EXTERNAL_SYSTEM_NAME=WinPassphrase -> configurable
uidToLowerCase=false
principal="HTTP/emma2.helena.gr@HELENA.GR";
};

com.ibm.security.jgss.initiate
{
com.ibm.security.auth.module.Krb5LoginModule required;
};
com.ibm.security.jgss.accept
{
com.ibm.security.auth.module.Krb5LoginModule required
debug=false
credsType=acceptor
```

```
useKeytab="/opt/siemens/krb5.keytab"
principal="HTTP/emma2.helena.gr@HELENA.GR";
};
2. File /opt/siemens/HiPathCA/config/common/
authentication.cfg

com.siemens.ca.server.config.jaas.appName=SSOLogin
com.siemens.ca.server.config.jaas.showLoginDialog=true |
false -> configurable item
```

6.21.7.3 SPNEGO IAE only Configuration

1. File /opt/siemens/common/conf/krb5-jaas_ibm.conf

```
/**
 * JAAS configuration for JGSS in an IBM JRE.
 * Modify the entries to suit your environment.
 */

com.ibm.security.jgss.accept {
com.ibm.security.auth.module.Krb5LoginModule required
debug=false
doNotPrompt=true
credsType=acceptor
useKeytab="FILE:/opt/siemens/common/conf/krb5.keytab"
storeKey=true
principal="HTTP/Emma.helena.gr@helena.gr";
};

com.ibm.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required
debug=false;
};

2. SPNEGO IAE service instance file
/opt/siemens/common/conf/config-beans/instance_461663ba-f4b5-479f-
b805-8dcba7a01e43.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstanceData className="com.siemens.symphonia.spnegoiae.impl.SpnegoIaeImpl"
  displayName="SPNEGO IAE service" enabled="true" guid="461663ba-f4b5-479f-
b805-8dcba7a01e43" version="1.0.0">
<Property name="ServicePrincipalName" value="HTTP/Emma.helena.gr@HELENA.GR"/
Import Sample for realm HELENA.GR:

##ExternalId;externalId;assignedUserIdentity;assignedExternalSystemId;
isContactMaster;isProvisioningMaster;additionalInfo
ExternalId;mSample;mSample@system;HELENA.GR;false;false;
ExternalId;tBrown;tBrown@system;HELENA.GR;false;false;
```

6.21.8 Support of Single Sign On (SSO) for multiple Domains

In V11 it is possible to have the Single Sign On (SSO) feature for more than one domain. Background is that SOAP does not address anymore port 4709 by any

OpenScape UC Clients, thus OpenScape UC supports more Key Distribution Center (KDC) domains.

In order to support more KDC domains perform the following steps:

- 1) Create for each KDC an individual `krb5.keytab` file and provide a unique name.
- 2) Install the `krb5-client` package on the Backend Server: #

```
rpm -ivh krb5-client-a.b.c-d.e.x86_64
```



```
e.g. rpm -ivh krb5-client-1.12.1-19.1.x86_64
```
- 3) Copy all `krb5.keytab` files to the Backend Server.
- 4) Use the program `ktutil` in order to concatenate all the individual `krb5.keytab` files to one single `krb5.keytab` file.

```
# ktutil
ktutil: read_kt /root/krb5.keytab-1
ktutil: read_kt /root/krb5.keytab-2
ktutil: read_kt /root/krb5.keytab-3
ktutil: write_kt /opt/siemens/krb5.keytab
ktutil: quit
```

NOTICE: Take care to the sequence of the various `krb5.keytab` files. The various PRINCIPALS must be configured in the `jaas.cfg` file in the same order.

- 5) Verify the content of the new `krb5.keytab` file:

```
# klist -k /opt/siemens/krb5.keytab
Keytab name: FILE:/root/krb5.keytab
KVNO Principal
----
-----
3      HTTP/openscapeuc.unify.admin@UNIFY.ADM1
3      HTTP/openscapeuc.unify.admin@TRAINING17.NET
3      HTTP/openscapeuc.unify.admin@APT.net
```

extend the file `jaas.cfg` with the SSO Configuration or add the missing configuration:

```
SSOLogin
{
com.siemens.ca.security.auth.winsso.SPNEGOKrbLogin
required
    useSharedState=false
    converterClass="com.siemens.ca.security.auth.UidResolver"
    EXTERNAL_SYSTEM_NAME=WinPassphrase
    uidToLowerCase=false
    principal1="HTTP/<FQDN-FE>@<Domain-1>"
    principal2="HTTP/<FQDN-FE>@<Domain-2>"
    principal3="HTTP/<FQDN-FE>@<Domain-3>";
};
com.ibm.security.jgss.initiate
{
com.ibm.security.auth.module.Krb5LoginModule required;
};
com.ibm.security.jgss.accept
```

```
{
com.ibm.security.auth.module.Krb5LoginModule required
    debug=true
    credsType=acceptor
    useKeytab="/opt/siemens/krb5.keytab"
    principal="HTTP/<FQDN-FE>@<Domain-1>";
com.ibm.security.auth.module.Krb5LoginModule required
    debug=true
    credsType=acceptor
    useKeytab="/opt/siemens/krb5.keytab"
    principal="HTTP/<FQDN-FE>@<Domain-2>";
com.ibm.security.auth.module.Krb5LoginModule required
    debug=true
    credsType=acceptor
    useKeytab="/opt/siemens/krb5.keytab"
    principal="HTTP/<FQDN-FE>@<Domain-3>";
};
<FQDN-FE> =
```

- UC APP Server for Small Deployment
- UC Frontend for Large Deployment with 1 OS UC FE
- Load Balancer for Large Deployment with more than 1 OS UC FE

6) Restart the OpenScape UC WebClient

```
# /etc/init.d/symphoniad restart WebClient
```

6.22 Configuring the Use of Windows Login Data

NOTICE: Starting with UC V11R5 FR9, the Java runtime environment has been updated. Single Sign-On configuration requires **Kerberos AES 256 bits encryption**. Legacy encryption methods (such as RC4 and DES) are no longer supported.

This chapter provides information about the following topics:

- [Concept of Using Windows Login Data](#)
- [Configuring the Use of Windows Login Data without simultaneous Use of SSO for OpenScape Web Client](#)
- [Configuring the Use of Windows Login Data with simultaneous Use of SSO for OpenScape Web Client](#)

6.22.1 Concept of Using Windows Login Data

Using Windows login data enables Windows users to log on to the OpenScape Mobile Client with the Windows login name and Windows password.

6.22.2 Configuring the Use of Windows Login Data without simultaneous Use of SSO for OpenScape Web Client

If you do not wish to use Single Sign-On for OpenScape Web Client simultaneously, execute the following steps to configure the use of Windows login data:

- 1) [Activating the Windows Authentication](#)
- 2) [Changing the Kerberos Configuration File](#)
- 3) [Creating User Assignments](#)
- 4) [Importing User Assignments](#)
- 5) [Restarting OpenScape UC Application](#)

These steps are described in detail in the following sections.

6.22.2.1 Activating the Windows Authentication

OpenScape Mobile Client users cannot log on to OpenScape UC Application with their Windows login data until the Windows authentication has become active system-wide.

How to activate the Windows authentication system-wide:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Security – Passphrase Login Service** component and click on the associated component name.

The dialog with the settings of the relevant component opens.

- 6) Enter value **true** in the **WindowsPassphraseAuthentication** field.
- 7) Select **Save** to copy the new settings.

The Windows authentication is now active within the entire system.

6.22.2.2 Changing the Kerberos Configuration File

Using Windows login data is based on the authentication protocol Kerberos. To adjust the Kerberos implementation of OpenScape UC Application to the

existing system environment, you need to reconfigure the relevant configuration file of the application computer (active and possibly passive one).

How to change the Kerberos configuration file:

- 1) Open the following configuration file with a text editor:

`wpa_krb5.conf`

You find this file in the following folder of the application computer:

`<Osc-Install70>/common/conf/`

- 2) Specify in the **[realms]** section the Windows domain used and assign it with parameter **kdc** the IP address and port of its respective key distribution center.

NOTICE: If the host name of the associated computer system can be resolved into an IP address in the network, you can also enter the associated host name instead of the IP address.

Use only capital letters for the domain names of the realm.

Examples of the COMPANY.COM realm domain:

```
[realms]
COMPANY.COM = {
    kdc = domkdc.company.com:88
    kdc = domctl.company.com:88
}
```

...

NOTICE: Windows supports under `[realms]` a single entry only. Environments that require a second realms entry are not supported on the operating system side.

- 3) Specify in section **[libdefaults]** for **default_realm** the desired name for the Kerberos realm used by default. In doing so, use capital letters only.

Example:

```
[libdefaults]
default_realm = COMPANY.COM
kdc_timeout = 30000
...
```

- 4) If you specified several kdc entries in step 2, configure value 2000 for the `kdc_timeout` parameter.

This will give the system time to send a request to further Key Distribution Centers if the first Key Distribution Center on the list does not answer.

- 5) Save the changes in the configuration file.

You have thus changed the Kerberos configuration file.

⁷⁰ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

6.22.2.3 Creating User Assignments

For using Windows login data trouble-free, you need to assign the name of the respectively associated Windows user account to the relevant OpenScape user accounts. Import the corresponding user assignments in OpenScape UC Application for this purpose.

Before you can import the user assignments in OpenScape UC Application you need to create the relevant assignments.

How to create the user assignments:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.

The dialog for exporting configurations opens.

- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.
- 8) Open the downloaded Zip file and open the following Zip file contained therein:

Package_domainmanagement_domainmanagement001.zip

- 9) In there open the following file with a text editor:

domain_configuration.csv

NOTICE: You should use the text editor Notepad++. If you use other text editors you need to make sure that no Byte-Order-Mark – BOM is used.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the user assignments under the entry that begins with **##ExternalId**.
 - The fields of an entry are separated from each other by semicolon.
- 10) Look for the user assignments section in the file. This section begins with the following line:

##ExternalId;externalId;isContactMaster ...

- 11) Remove all lines that do not belong to the user assignments section from the file.

In a file without existing user assignment, only the following line then remains:

```
##ExternalId;externalId;isContactMaster ...
```

- 12) Add to the file under `##ExternalId` all required user assignments that assign the respectively associated Microsoft Exchange user account to the relevant OpenScope user accounts.

In doing so please heed the following:

- The following data special characters must be marked by the escape character \ for later import: , \ # =
- Create a new ExternalId entry for each assignment.
- Enter the reserved name **ExternalId** under **##ExternalId**.

This name defines the entry as user assignment.

- Enter the Windows login ID of the relevant OpenScope user account under **externalId**. In doing so, use the @-notation and heed case sensitivity.

Use only capital letters for the domain name.

Example: mSample@COMPANY.COM

- Always specify the **true** value under **isContactMaster**.
- Always specify the **false** value under **isProvisioningMaster**.
- Enter the expression **WinPassphrase** under **assignedExternalSystemId**.
- Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: mSample@system

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

##ExternalId	externalId	isContactMaster	isProvisioningMaster
ExternalId	mSample@COMPANY.COM	true	false
ExternalId	tBrown@COMPANY.COM	true	false
...	...	...	...

assignedExternalSystemId	assignedUserIdentity	
WinPassphrase	mSample@system	
WinPassphrase	tBrown@system	
...	...	

```
##ExternalId;externalId;isContactMaster;  
isProvisioningMaster;assignedExternalSystemId;  
assignedUserIdentity  
  
ExternalId;mSample@COMPANY.COM;true;false;WinPassphrase;  
mSample@system  
  
ExternalId;tBrown@COMPANY.COM;true;false;WinPassphrase;  
tBrown@system  
...
```

- 13) Save the supplemented file under the name `domain_configuration.csv` in CSV format.
- 14) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

You have now created the required user assignments.

6.22.2.4 Importing User Assignments

You need to import the user assignments just created in OpenScape UC Application.

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.
The dialog for importing a configuration opens.
- 4) In the **Import file** field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file.
- 5) Click on **Next**.
- 6) Check that the **Common Management Platform** option has been selected under **Type of file to be imported**.
- 7) Check that the **Domain Management** option has been selected under **Included type of data**.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

You have now imported the user assignments in OpenScape UC Application.

6.22.2.5 Restarting OpenScape UC Application

You need to reboot OpenScape UC Application for the performed settings to take effect.

Reboot OpenScape UC Application by executing the following commands:

```
/etc/init.d/symphoniad stop
```

```
/etc/init.d/symphoniad start
```

All settings for using Windows login data are now effective.

6.22.3 Configuring the Use of Windows Login Data with simultaneous Use of SSO for OpenScape Web Client

If you wish to use Single Sign-On for OpenScape Web Client also, execute the following steps to configure the use of Windows login data:

- 1) [Activating the Windows Authentication](#)
- 2) [Determining Configuration Files used](#)
- 3) [Creating User Assignments](#)
- 4) [Importing User Assignments](#)
- 5) [Restarting OpenScape UC Application](#)

These steps are described in detail in the following sections.

NOTICE: We assume that you have already configured Single Sign-On for OpenScape Web Client (see [Configuring SSO \(Single Sign-On\)](#) on page 514).

6.22.3.1 Activating the Windows Authentication

Users of the OpenScape Mobile Client cannot log on to OpenScape UC Application with their Windows login data until the Windows authentication has become active system-wide.

How to activate the Windows authentication system-wide:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Security – Passphrase Login Service** component and click on the associated component name.

The dialog with the settings of the relevant component opens.

- 6) Enter value **true** in the **WindowsPassphraseAuthentication** field.
- 7) Select **Save** to copy the new settings.

The Windows authentication is now active within the entire system.

6.22.3.2 Determining Configuration Files used

OpenScape UC Application deploys the following configuration files for using Windows login data by default:

JAAS configuration: `wpa_jaas.conf`

Kerberos configuration: `wpa_krb5.conf`

If Single Sign-On is already configured for OpenScape Web Client, the files configured for Single Sign-On must be deployed instead of these default configuration files. Such files are:

JAAS configuration: `jaas.conf`

Kerberos configuration: `krb5.conf`

Execute the following steps to determine the configuration files to be used instead of the default configuration files:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Windows Passphrase Authentication Component** and click on the associated component name.

The dialog with the settings of the relevant component opens.

- 6) Specify in the **JAASConfigFile** field the file in which you have configured JAAS for Single Sign-On of the OpenScape Web Client. This is the following file by default:

jaas.cfg

You find this file in the following folder of the computer system for which Single Sign-On has been configured:

<Osc-Install⁷¹>/HiPathCA/config/common/

- 7) Specify in the **KRB5ConfigFile** field the file in which you have configured Kerberos for Single Sign-On of the OpenScape Web Client. This is the following file by default:

Krb5.conf

You find this file in the following folder of the computer system for which Single Sign-On has been configured:

<Osc-Install>/common/conf/

- 8) Select **Save** to copy the new settings.
- 9) Due to an error that occurs with initializing services in the Windows operating system, you must copy the settings from the krb5.conf file to the wpa_krb5.conf file also.

You find the wpa_krb5.conf file in the same folder of the application computer as the krb5.conf file.

You have thus determined the JAAS and Kerberos configuration file used.

6.22.3.3 Creating User Assignments

For using Windows login data trouble-free, you need to assign the name of the respectively associated Windows user account to the relevant OpenScape user accounts. Import the corresponding user assignments in OpenScape UC Application for this purpose.

Before you can import the user assignments in OpenScape UC Application you need to create the relevant assignments.

How to create the user assignments:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.
- The dialog for exporting configurations opens.
- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.

⁷¹ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.
- 8) Open the downloaded Zip file and open the following Zip file contained therein:

Package_domainmanagement_domainmanagement001.zip

- 9) In there open the following file with a text editor:

domain_configuration.csv

NOTICE: You should use the text editor Notepad++. If you use other text editors you need to make sure that no Byte-Order-Mark – BOM is used.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the user assignments under the entry that begins with `##ExternalId`.
 - The fields of an entry are separated from each other by semicolon.
- 10) Look for the user assignments section in the file. This section begins with the following line:

```
##ExternalId;externalId;isContactMaster ...
```

- 11) Remove all lines that do not belong to the user assignments section from the file.

In a file without existing user assignment, only the following line then remains:

```
##ExternalId;externalId;isContactMaster ...
```


- 12) Add to the file under `##ExternalId` all required user assignments that assign the respectively associated Microsoft Exchange user account to the relevant OpenScape user accounts.

In doing so please heed the following:

- The following data special characters must be marked by the escape character `\` for later import: `, \ # =`
- Create a new `ExternalId` entry for each assignment.
- Enter the reserved name **ExternalId** under **##ExternalId**.

This name defines the entry as user assignment.

NOTICE: The ExternalID can be also modified in corresponding ExternalID tab in CMP

- Enter the Windows login ID of the relevant OpenScape user account under **externalId**. In doing so, use the `@`-notation and heed case sensitivity.

Use only capital letters for the domain name.

Example: `mSample@COMPANY.COM`

- Always specify the **true** value under **isContactMaster**.
- Always specify the **false** value under **isProvisioningMaster**.
- Enter the expression **WinPassphrase** under **assignedExternalSystemId**.
- Specify under **assignedUserIdentity** the information that is contained in the field of the same name of the relevant user's contact entry.

Example: `mSample@system`

NOTICE: The field sequence in the following examples may deviate from the field sequence in your system. In this case, arrange the settings as defaulted by your system.

User assignment examples:

<code>##ExternalId</code>	<code>externalId</code>	<code>isContactMaster</code>	<code>isProvisioningMaster</code>	...
<code>ExternalId</code>	<code>mSample@COMPANY.COM</code>	<code>true</code>	<code>false</code>	...
<code>ExternalId</code>	<code>tBrown@COMPANY.COM</code>	<code>true</code>	<code>false</code>	...
...	...	...	...	...

<code>assignedExternalSystemId</code>	<code>assignedUserIdentity</code>
<code>WinPassphrase</code>	<code>mSample@system</code>
<code>WinPassphrase</code>	<code>tBrown@system</code>
...	...

```
##ExternalId;externalId;isContactMaster;
isProvisioningMaster;assignedExternalSystemId;
assignedUserIdentity
```

```
ExternalId;mSample@COMPANY.COM;true;false;  
WinPassphrase;mSample@system
```

```
ExternalId;tBrown@COMPANY.COM;true;false;  
WinPassphrase;tBrown@system
```

...

- 13) Save the supplemented file under the name `domain_configuration.csv` in CSV format.
- 14) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.

You have now created the required user assignments.

6.22.3.4 Importing User Assignments

You need to import the user assignments just created in OpenScape UC Application.

How to import the user assignments:

- 1) Select in the CMP toolbar in the **Domain** drop-down list the domain the users of which are contained in the import file.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Import** in the navigation tree.

The dialog for importing a configuration opens.

- 4) In the **Import file** field specify the name of the import file (*.csv or *.zip). Enter the name and path or use the **Browse** button to select the file.
- 5) Click on **Next**.
- 6) Check that the **Common Management Platform** option has been selected under **Type of file to be imported**.
- 7) Check that the **Domain Management** option has been selected under **Included type of data**.
- 8) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

You have now imported the user assignments in OpenScape UC Application.

6.22.3.5 Restarting OpenScape UC Application

You need to reboot OpenScape UC Application for the performed settings to take effect.

Reboot OpenScape UC Application by executing the following commands:

```
/etc/init.d/symphoniad stop
```

```
/etc/init.d/symphoniad start
```

All settings for using Windows login data are now effective.

6.23 Controlling Busy Signaling (Busy-on-Busy)

This chapter provides information about the following topics:

- [Busy Signaling \(Busy-on-Busy\) Concept](#)
- [Activating Busy-on-Busy](#)

6.23.1 Busy Signaling (Busy-on-Busy) Concept

The busy signaling for devices is controlled for the whole system by the Busy-on-Busy setting.

By default, OpenScape UC Application uses for incoming calls a workflow in which the devices on a list are called one by one following the order of the list until the call is answered on one of these devices within a default time (RNA Time Out). If one of these devices is engaged, it is skipped in the workflow, and the workflow continues with the next device. If the call is answered on none of the devices, the call is routed to the voice mail box of the called OpenScape user.

In this default behavior, the caller will always see the ONS number of the called OpenScape user.

The system wide Busy-on-Busy setting modifies this workflow so that an engaged device is not skipped. The call is routed instead to the engaged device and the caller hears a busy signal.

In this case, the caller sees the ONS number of the called OpenScape user.

The busy signaling control via the Busy-on-Busy setting functions also with OpenScape users whose devices are part of an E / A Cockpit or call center solution.

If the engaged device is a mobile phone, the busy signaling control via the Busy-on-Busy setting functions only if the relevant provider signals the busy status to the OpenScape UC Application.

6.23.2 Activating Busy-on-Busy

The Busy-on-Busy setting provides system wide busy signaling control for engaged phone devices.

Start the configuration

How to activate the system wide Busy-on-Busy feature:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Personal Workflow Controls Factory Component** component and click on the associated component name.

The dialog with the settings of the component opens.

- 6) Specify the **true** value under **BusyOnBusy**.

- 7) Click on **Save** to copy the settings.

Starting with V11R1, OpenScape 4000 provides the interface for UC Busy-on-Busy.

- 1) OS4K CSTA Offered Event is enhanced with the **onsCall** parameter in private data as follows:

- No call associated with the UC user/ONS
 - CSTA Offered Event with no private data
- At least one call associated with the UC user/ONS (x calls)
 - CSTA Offered Event with private data onsCall = x

- 2) Activation in OS4K RMX (only for V11R1):

- CHANGE-ZANDE:TYPE=OPTFEA,OPTFEA=A,FEANUM=728;

- 3) Activation in OS4K CSTA CA4000:

- The "ENABLE_ONS"CALLS" parameter can be used to activate/deactivate reporting number of calls in CSTA Offered Event for an UC user.

- 4) The minimum software requirements for complete feature activation are the following:

- UC 10.4.6.0
- OS4K CSTA V11 R1.34.2
- OS4K RMX V11 R1.34.6

6.23.3 Busy on Busy for ONS incoming call

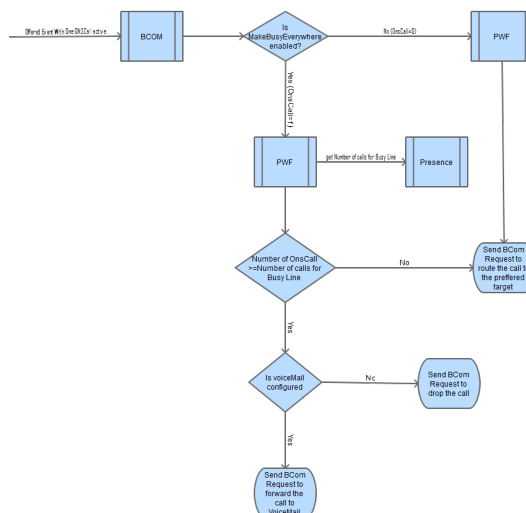
UC allows an administrator to configure users that are on a UC-initiated or ONS call not to receive further calls, regardless of the device actually used for the call(s). Subsequent inbound calls get “busy” treatment.

UC supports a global parameter called MakeBusyEverywhere which is OFF by default but when turned on, shall cause any inbound ONS call to a user whose device presence state is busy to be rejected with cause busy.

NOTICE: It is understood and intended that the “Number of calls for busy line” user-set able parameter impacts this feature, i.e. if a user sets this parameter to 2, ONS calls to him/her will only be rejected if he/she already has two active ONS calls.

NOTICE: If Voicemail is assigned to the user, call is redirected to Voice Mail Server (VMS) instead of busy.

NOTICE: This feature is supported by UC with OpenScope Voice and OpenScope 4000.



There are two modifiable parameters:

- MAKE_BUSY_EVERYWHERE

Default value is OFF.

In case you need this enabled, then the value must be set manually to ON

- NumberOfCallsForBusyLine

Default value is 2

The related configuration (XML) files are located in directory /opt/siemens/common/conf/config-beans.

How to find the file for changing the MAKE_BUSY_EVERYWHERE:

```
cd /opt/siemens/common/conf/config-beans
grep AddressManagerImpl instance*
```

sample output:

```
instance_f5cafa09-74f9-46ae-830e-729eace46bde.xml:<InstanceData  
className="com.siemens.symphonia.bcom.addressmanager.impl.AddressManagerImpl"  
displayName="Addressmanager component" enabled="true"  
guid="f5cafa09-74f9-46ae-830e-729eace46bde" version="1.0.0"
```

So the file is in this example is:

"instance_f5cafa09-74f9-46ae-830e-729eace46bde.xml".

NOTICE: grep returns <filename>:<returned line containing text>

How to find the file for modifying the NumberOfCallsForBusyLine:

```
cd /opt/siemens/common/conf/config-beans grep -in busy *
```

sample

```
output: instance_1137593a-a3ac-4661-a8c7-78cd38fa2ea7.xml:3: <Property  
name="BusyOnBusy" value="false" writable="true"/>
```

```
instance_1137593a-a3ac-4661-a8c7-78cd38fa2ea7.xml:9: <Property  
name="NumberOfCallsForBusyLine" value="2" writable="true"/>
```

```
instance_f5cafa09-74f9-46ae-830e-729eace46bde.xml:8: <Property  
name="MAKE_BUSY_EVERYWHERE" value="OFF"/>
```

NOTICE: When you set the flag -n in the grep command you get also the line number in which the text is located.
<filename>:<line number>:<returned line containing text>

IMPORTANT: With this command you see also if BusyOnBusy is activated and the information about status of MAKE_BUSY_EVERYWHERE. In order to activate "Busy On Busy" please refer to [Activating Busy-on-Busy](#) on page 559

Then you can edit the file(s) with a text editor, e.g. vi.

After you have adapted / modified the file(s) a restart of the UC system is required in order the changes to take affect.

IMPORTANT: "No ONS routing to DSS-D calls" feature takes precedence of "Busy on Busy" thus a DSS-D call will always be accepted without checking the requirements of the Busy-on-Busy feature.

IMPORTANT: There are several features interworking with the "Busy on Busy" feature so that in some cases the call never reaches the ONS, such features are e.g. Voicemail resource, CFW on busy on the OSV side, Controlling Busy Signaling.

6.23.4 Busy on Busy for Microsoft Teams Presence

You can configure OpenScape UC to enable the Busy on Busy functionality, according to user's presence in Microsoft Teams.

NOTICE: This feature is supported by OpenScape UC with OpenScape Voice and OpenScape 4000.

As a system administrator, you can enable or disable Busy on Busy for Microsoft Teams via the **USER_TEAMS_BUSY** parameter.

The default value is **OFF**:

```
<Property name="USER_TEAMS_BUSY" value="OFF"/>
```

To modify the value of the **USER_TEAMS_BUSY** parameter, follow the steps below:

- 1) Navigate to the following path:
`cd /opt/siemens/common/conf/config-beans`
- 2) Use the `grep` command to locate the file that contains the **USER_TEAMS_BUSY** parameter:
`grep AddressManagerImpl instance*`

Sample output:

```
instance_f5cafa09-74f9-46ae-830e-729eace46bde.xml:<InstanceData  
className="com.siemens.symphonia.bcom.addressmanager.impl.AddressManagerImpl" displayName="Addressmanager component"  
enabled="true"  
  guid="f5cafa09-74f9-46ae-830e-729eace46bde"  
version="1.0.0"
```

In this example, the file that needs to be modified is:
`instance_f5cafa09-74f9-46ae-830e-729eace46bde.xml`.

NOTICE: The `grep` command returns the following output:
`<filename>:<returned line containing text>`

- 3) Set the value of the **USER_TEAMS_BUSY** parameter to the desired value:
 - OFF - the parameter is disabled.
 - ON - the parameter is enabled.
- 4) Save the changes in the configuration file, then restart the OpenScape UC system for the changes to take effect.

6.24 Executing Application Operations for OpenScape UC Application

You can start selected features for the CMP application OpenScape UC Application from within the CMP.

Such features are:

- Software activation
- Restarting all computer systems of OpenScape UC Application

Start the configuration

How to select a feature for the application OpenScape UC Application from within the CMP:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Applications**.
A list of all applications available in the entire system is displayed in the workspace.
- 3) Click on  in the list entry of the **OpenScape UC** application to open the component's actions menu.
- 4) Select the desired action from the action menu:
 - **Software activation** Is used to activate software patches, for example. You find details about using this feature in the *OpenScape UC Application, Installation and Upgrade* manual.
 - **Restart OpenScape UC** Reboots all OpenScape UC Application computer systems.

Please heed warnings that point out effects of a restart.

6.25 Further administrative Tasks

This chapter provides information about the following topics:

- [Configuring a reduced OpenScape Voice Assistant](#)
- [Starting/restarting OpenScape UC Application](#)
- [Saving the Security Certificate for the CMP](#)
- [Checking the Availability of CSTA Connections](#)
- [Checking the CSTA Connection Function](#)
- [Changing the User Passwords Policies](#)
- [Changing Policies for User PINs](#)
- [Synchronizing License Assignments anew](#)
- [Creating a Firewall Rule in OpenScape Voice](#)
- [Changing IP Addresses / FQDNs of the UC Application Computer Systems](#)
- [Configuring the IPv6 Support for OpenScape Media Server](#)
- [Configuring the HTTPS Port for CMP Access](#)
- [Activating HTTP Port for Framework](#)
- [Activating the anonymized Originator Address for automatic e-mails](#)
- [Configuring Scheduled Message Routing](#)
- [Transmitting Information about OpenScape 4000 Resources to OpenScape UC Application](#)
- [Activating the Call Acceptance for remote preferred Devices](#)
- [Managing Network Address \(NAT\) Translations](#)
- [Suppressing Features for managing preferred Devices in the Clients](#)
- [Starting all Conferences as Video Conference](#)
- [Copying an OpenScape Voice Resource with changed Subscriber Type](#)
- [Configuring the Status Monitoring for OpenScape Voice Multiline Hunt Groups \(MLHG\)](#)
- [Restricting the Visibility of Contacts based on Groups](#)
- [Changing the Service Account for UC Application Services](#)

6.25.1 Configuring a reduced OpenScape Voice Assistant

If in an OpenScape system, the OpenScape components are distributed on several computer systems, it is not necessary to install with the CMP a complete OpenScape Voice Assistant on each of the computer systems. It is sufficient to use a complete OpenScape Voice Assistant on only one of the computer systems. On all other computer systems, only parts of the OpenScape Voice Assistant are required.

In this case, the OpenScape Voice system of the OpenScape system can only be configured and managed via the CMP the complete OpenScape Voice Assistant has been installed with.

NOTICE: A reduced OpenScape Voice Assistant is always configured based on a complete OpenScape Voice Assistant. For this reason, you must always install a complete OpenScape Voice Assistant first on the relevant computer system before configuring a reduced OpenScape Voice Assistant. This is accomplished during the normal installation process described in the OpenScape UC Application installation manual.

Start the configuration

How to configure a reduced OpenScape Voice Assistant on an OpenScape computer system:

- 1) Execute the following command on the computer system where you would like to use only a reduced OpenScape Voice Assistant.

```
zypper in HiPathAssistantSync
```

You will be guided through the configuration in the following way. You must enter the bold-highlighted values where indicated.

```
Restoring system sources...
/repodata/repomd.xml (dir:///root/rpmrepo/) is unsigned,
continue? [y/n]: y
Parsing metadata for http://10.1.253.250/sources/
SLES-12-SP4-x86...
Parsing metadata for dir:///root/rpmrepo/...
Parsing RPM database...
```

```
2 Problems:
```

```
Problem: Cannot install
HiPathAssistantSync-1.0-1.noarch[dir:///root/rpmrepo/]
because it is conflicting with HiPathAssistant
Problem: HiPathAssistant-1.0-1.noarch is locked and
cannot be uninstalled.
```

```
Problem: Cannot install
HiPathAssistantSync-1.0-1.noarch[dir:///root/rpmrepo/]
because it is conflicting with HiPathAssistant
A conflict over HiPathAssistantSync == 1.0-1
(HiPathAssistantSync) requires the removal of to-be-
installed HiPathAssistantSync-1.0-1.noarch[dir:///root/
rpmrepo/]
```

```
Solution 1: do not install HiPathAssistantSync
do not install HiPathAssistantSync-1.0-1.noarch[dir:///
root/rpmrepo/]
Solution 2: delete HiPathAssistant
delete HiPathAssistant-1.0-1.noarch
Solution 3: Ignore this conflict of HiPathAssistantSync
number, (r)etry or (c)ancel> 2
Applying solution 2
```

```
Problem: HiPathAssistant-1.0-1.noarch is locked and
cannot be uninstalled.
```

```
Solution 1: unlock HiPathAssistant
Solution 2: unlock all resolvables
Solution 3: keep HiPathAssistant keep
HiPathAssistant-1.0-1.noarch
number, (r)etry or (c)ancel> 2
Applying solution 2
```

```
1 Problems:
Problem: c-1.0-1.noarch has missing dependencies
```

```
Problem: c-1.0-1.noarch has missing dependencies
There are no alternative installed providers of
HiPathAssistant for c-1.0-1.noarch
```

```
Solution 1: keep HiPathAssistant
keep HiPathAssistant-1.0-1.noarch
Solution 2: delete c
delete c-1.0-1.noarch
Solution 3: Ignore this requirement just here
Solution 4: Ignore this requirement generally
number, (r)etry or (c)ancel> 3
Applying solution 3
```

```
Summary:
<install> [S2:0]
[package]HiPathAssistantSync-1.0-1.noarch
<uninstall> [S0:0][package]HiPathAssistant-1.0-1.noarch
Continue? [y/n]: y
Removing: [S0:0][package]HiPathAssistant-1.0-1.noarch
Downloading: [S2:0]
[package]HiPathAssistantSync-1.0-1.noarch,
1.3 K(0 B unpacked)
Installing: [S2:0]
[package]HiPathAssistantSync-1.0-1.noarch
```

The original OpenScape Voice Assistant of the computer system has now only the functions of a reduced OpenScape Voice Assistant.

NOTICE: To migrate a reduced OpenScape Voice Assistant to a complete OpenScape Voice Assistant, uninstall the RPM package AssistantSync and reinstall the OpenScape Voice Assistant.

6.25.2 Starting/restarting OpenScape UC Application

NOTICE: A start / reboot of OpenScape UC Application merely starts / reboots the associated UC Application services but not the associated computer system.

NOTICE: Openfire and Facade/HAProxy servers do not depend on the other UC nodes in terms of the order in which they should be started.

When starting or rebooting OpenScape UC Application please heed the following:

- You can start and stop the services of a single application computer, front-end computer or Media Server computer at will as long as the services of all other UC Application computer systems remain started.
- If you wish to restart the UC Application services of several computer systems, you can stop them in any sequence or simultaneously.

Recommend sequence:

Stop Deployment

Stop all application computers in any sequence or simultaneously, but not the Application Computer, which must be stopped last. Start Deployment

- 1) Start Application Computer first and monitor BE CPU resources to be under 100% in order to continue with the rest of the UC application Servers.
- 2) Start Media Server computers one by one, after verifying BE resources are low.
- 3) Start FrontEnd Server computers at any sequence or simultaneously.

For Large / Very Large deployments the above steps should be performed in above mentioned order.

- If you wish to start the UC Application services of several computer systems and the application computer is among them, we urgently recommend to start the application computer before the other computer systems. This enables the other UC Application services to access the OpenScape UC Application database when they are started at a later date. After you have started the application computer services, you need to wait for a minute before you boot the services of the other UC Application computer systems in any sequence or simultaneously.

Recommended Sequence: Start Deployment

- 1) Start Application Computer first and monitor BE CPU resources to be under 100% in order to continue with the rest of the UC application Servers.
- 2) Start Media Server computers one by one, after verifying BE resources are low.
- 3) Start FrontEnd Server computers at any sequence or simultaneously.

For Large / Very Large deployments the above steps should be performed in above mentioned order.

- If you wish to start the UC Application services of several computer systems and the application computer is not among them, you can start them in any sequence or simultaneously.

Recommended Sequence:

Start Deployment

- 1) Start Application Computer first and monitor BE CPU resources to be under 100% in order to continue with the rest of the UC application Servers.
- 2) Start Media Server computers one by one, after verifying BE resources are low.
- 3) Start FrontEnd Server computers at any sequence or simultaneously. For Large / Very Large deployments the above steps should be performed in above mentioned order.

The same rules apply if you do not only want to start / reboot the UC Application services but the relevant computer systems completely.

The OpenScape UC Application reboot differentiates the following scenarios:

- [Rebooting the UC Application Services of a Computer System](#)
- [Rebooting UC Application Services of all Computer Systems](#)

6.25.2.1 Rebooting the UC Application Services of a Computer System

How to reboot the UC Application services of a selected computer system:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.
A list of all system nodes and external links available in the entire system is displayed in the workspace.
- 3) Click on  in the list entry of the system node the UC Application services of which you wish to reboot for opening the node's action menu.
- 4) In the action menu, select **Restart Node**.
A security prompt points out the consequences of a reboot.
- 5) To execute the reboot of the selected UC Application services, confirm the security prompt with **OK**.

All UC Application services of the selected system node are stopped and immediately rebooted.

6.25.2.2 Rebooting UC Application Services of all Computer Systems

How to reboot the UC Application services of all computer systems with keeping the necessary starting order automatically:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Applications**.
A list of all applications available in the entire system is displayed in the workspace.

- 3) Click on  in the list entry of the **OpenScapeUC** application to open the application's actions menu.
- 4) In the actions menu, select **Restart OpenScape UC**.
A security prompt points out the consequences of a reboot.
- 5) To execute the reboot of all UC Application services, confirm the security prompt with **OK**.

All users are automatically logged off from the CMP and the UC Application services of all computer systems stop and restart.

NOTICE: You can reboot the UC Application services of all computer systems also via a shell. The following script exists for this purpose: `largeDeployRestart.sh` You find details about this script in the manual *OpenScape UC Application, Installation and Upgrade, Setup Guide*.

6.25.3 Saving the Security Certificate for the CMP

When you invoke the CMP, the web browser usually displays a security alarm that returns with every login.

The reason is that the security certificate of the CMP is issued by an institution that the web browser used does not trust.

You can avoid this security alarm after its first appearance by installing the security certificate of the CMP as trusted security certificate in the web browser used.

How to proceed is described in the *OpenScape Common Management - Platform, Administrator Documentation*.

6.25.4 Checking the Availability of CSTA Connections

NOTICE: The following description assumes the presence of the network analysis software *Tethereal* on the computer system of OpenScape Voice.

OpenScape UC Application must monitor and control the OpenScape Voice devices. Configure a CSTA link between OpenScape Voice and each UC Application server for this purpose.

During the system operation it may happen that some of these CSTA connections are not properly closed. This causes the number of possible CSTA connections to be unavailable although these links are not used anywhere.

You can use the network analysis software *tethereal* to check whether this case applies.

Start the configuration

How to check whether CSTA connections between OpenScape Voice and OpenScape UC Application have not been properly closed:

- 1) Execute the following command on the OpenScape Voice computer system:
`netstat -na|grep -i ":1040"`

As a result you see all connections currently configured.

Example:

```
tcp 0 0 10.75.80.115:1040 0.0.0.0:*  
LISTEN  
tcp 0 0 10.75.80.115:1040 129.103.29.44:58147  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.204:37438  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.204:36217  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.204:36216  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.204:36225  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.12:37084  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.12:37085  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.12:37078  
ESTABLISHED  
tcp 0 0 10.75.80.115:1040 129.103.29.12:37092  
ESTABLISHED
```

- 2) Execute the following command on the OpenScape Voice computer system:

```
tethereal -i any -R "tcp.dstport==1040"
```

As a result you see which connections are actually used.

Example:

```
tethereal: WARNING: Promiscuous mode not supported on  
the "any" device.  
Capturing on Pseudo-device that captures on all  
interfaces  
0.638240 129.103.29.204 -> 10.75.80.115 TCP 36216 >  
netarx [PSH, ACK] Seq=0 Ack=0  
  
Win=8576 Len=30 TSV=228217987 TSER=229338913  
0.640427 129.103.29.204 -> 10.75.80.115 TCP 36216 >  
netarx [ACK] Seq=30 Ack=210  
  
Win=8576 Len=0 TSV=228217989 TSER=229343916  
0.740348 129.103.29.12 -> 10.75.80.115 TCP 37084 >  
'netarx [PSH, ACK] Seq=0 Ack=0  
  
Win=8576 Len=30 TSV=768463170 TSER=229339015  
0.740859 129.103.29.12 -> 10.75.80.115 TCP 37084 >  
netarx [ACK] Seq=30 Ack=210
```

```
Win=8576 Len=0 TSV=768463171 TSER=229344017  
0.752139 129.103.29.12 -> 10.75.80.115 TCP 37085 >  
netarx [PSH, ACK] Seq=0 Ack=0
```

```
Win=23686 Len=30 TSV=768463182 TSER=229339027  
0.752596 129.103.29.12 -> 10.75.80.115 TCP 37085 >  
netarx [ACK] Seq=30 Ack=210
```

```
Win=23686 Len=0 TSV=768463182 TSER=229344029  
0.925178 129.103.29.12 -> 10.75.80.115 TCP 37078 >  
netarx [PSH, ACK] Seq=0 Ack=0
```

```
Win=8576 Len=30 TSV=768463355 TSER=229339200  
0.925747 129.103.29.12 -> 10.75.80.115 TCP 37078 >  
netarx [ACK] Seq=30 Ack=210
```

```
Win=8576 Len=0 TSV=768463355 TSER=229344202
```

The connections put out with **[ACK]** have not been properly closed – in our example thus 4 of altogether 10 connections.

- 3) If the number of available CSTA connections becomes too small, reboot OpenScape Voice to reset all connections.

You have now checked how many CSTA connections are actually still available for the CSTA communication.

6.25.5 Checking the CSTA Connection Function

OpenScape UC Application must monitor and control the OpenScape Voice devices. Configure a CSTA link between OpenScape Voice and each UC Application server for this purpose.

If required, you can check whether the CSTA connection between OpenScape UC Application and OpenScape Voice works correctly and OpenScape Voice devices are monitored.

Start the configuration

How to check whether the CSTA connection between OpenScape Voice and OpenScape UC Application works correctly:

Execute the following command on the application computer of OpenScape UC Application:

```
grep "] Monitor" symphonia.log
```

The ensuing output should resemble the following example:

```
2007-08-03 18:05:19,649 DEBUG
```

```
[com.siemens.symphonia.bcom.bcomsvc.impl.MonitorHandling]  
Monitor started for +498972210211
```

```
2007-08-03 18:05:19,650 INFO
```

```
[com.siemens.symphonia.bcom.bcomsvc.impl.MonitorHandling]  
Monitor to set for BCom 1 #+498972210204
```

```
2007-08-03 18:05:19,660 DEBUG
```

```
[com.siemens.symphonia.bcom.bcomsvc.impl.MonitorHandling]
```

Monitor started for +498972210204

You have now checked whether the CSTA connection between OpenScape Voice and OpenScape UC Application works correctly.

6.25.6 Changing the User Passwords Policies

To comply with the default requirements a user password must:

- comprise at least eight characters
- contain at least one capital letter
- contain at least one digit
- contain at least one special character
- contain each character not more than three times in succession

Furthermore, the following applies by default:

- Each user must change his/her password after 90 days at the next password-based login.

NOTICE: This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Login password never expires** option on the **Password / PIN** tab of the relevant user settings.

- A user must not enter an incorrect password more than five times. If this number is exceeded, his/her user account is automatically locked for password-based access.

Locking the password-based access does not influence the PIN-based access of the relevant user via telephone.

- The last five passwords of a user are stored in a password history. A user cannot configure a password that is contained in the password history.

You can adjust these policies, valid for the entire system, in the following XML file:

PassphrasePolicyConfig.xml

You find this file in the following folder of the computer system set up on OpenScape UC Application.

`<Osc-Install72>/common/conf/`

Extract from the file PassphrasePolicyConfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PassphrasePolicyConfig version="2.0">
  <PassphrasePolicy>
    <Type>pwd</Type>
    <MinimumAge>86400000</MinimumAge>
    <MaximumAge>777600000</MaximumAge>
    <MinimumLength>8</MinimumLength>
    <MaximumLength>0</MaximumLength>
```

⁷² `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`


```

        <MinimumDigits>1</MinimumDigits>
        <MinimumSpecialCharacters>1</MinimumSpecialCharacters>
        <MinimumUpperCaseCharacters>1</
MinimumUpperCaseCharacters>
        <MaximumRepeatedCharacters>3</
MaximumRepeatedCharacters>
        <MaximumFailedAttempts>5</MaximumFailedAttempts>
        <PasswordHistoryDepth>5</PasswordHistoryDepth>
        <LockoutTime>1800000</LockoutTime>
        <PeriodOfInactivity>90</PeriodOfInactivity>
        <MinimumChangedCharacters>3</MinimumChangedCharacters>
</PassphrasePolicy >
...

```

The following parameters of this XML file control the user password policies valid for the entire system.

- [MinimumAge](#)
- [MaximumAge](#)
- [MinimumLength](#)
- [MaximumLength](#)
- [MinimumDigits](#)
- [MinimumSpecialCharacters](#)
- [MinimumUpperCaseCharacters](#)
- [MaximumRepeatedCharacters](#)
- [MaximumFailedAttempts](#)
- [PasswordHistoryDepth](#)
- [LockoutTime](#)
- [PeriodOfInactivity](#)
- [MinimumChangedCharacters](#)

These settings have the following functions.

- **MinimumAge**

Specifies the period after a password alteration in which a user must not change his/her password again.

This period is only effective between two password modifications performed by a user himself/herself. If the administrator resets the user password, the relevant user can immediately change his/her password.

The set value is evaluated in milliseconds.

- **MaximumAge**

Specifies the period after which a user must change his/her password the next time he/she logs in.

This period is only effective between two password modifications performed by a user himself/herself. If the administrator resets the user password, the relevant user must only change his/her password if the **User has to change login password at next login** option of the user settings is also active.

If you set value **0**, you disable the automatic password alteration prompt.

The set value is evaluated in milliseconds.

NOTICE: This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Login**

password never expires option on the **Password / PIN** tab of the relevant user settings.

- **MinimumLength**

Specifies the number of characters a user password must at least consist of.

- **MaximumLength**

Specifies the number of characters a user password must not exceed. If you set value **0** this policy is not used.

- **MinimumDigits**

Specifies the number of digits a user password must at least contain. This number is included in the number of [MinimumLength](#) and [MaximumLength](#).

- **MinimumSpecialCharacters**

Specifies the number of special characters a user password must at least contain. This number is included in the number of [MinimumLength](#) and [MaximumLength](#).

- **MinimumUpperCaseCharacters**

Specifies the number of capital letters a user password must at least contain. This number is included in the number of [MinimumLength](#) and [MaximumLength](#).

- **MaximumRepeatedCharacters**

Specifies how often a letter, special character or digit may successively occur in the user password.

Example: The password *Schifffahrer* (German for skipper or boat passenger) is only valid if this parameter has at least been set to **3**. For, letter **f** appears in the password three times in a row.

If you set value **0** this policy is not used.

- **MaximumFailedAttempts**

Specifies how often a user may enter an incorrect password during the password-based login. If a user exceeds this number, his/her user account will automatically be locked for password-based access.

Locking the password-based access does not influence the PIN-based access of the relevant user via telephone.

If you set value **0** this policy is not used.

- **PasswordHistoryDepth**

Specifies how many of the last passwords are stored in the password history of each user. A user cannot configure a password that is contained in the password history.

The PIN history is administered independently from the password history.

This policy is not used when the administrator assigns a password to a user.

- **LockoutTime**

Specifies how long the password-based access is locked for a user if he/she has entered an incorrect password more often than is defined under [MaximumFailedAttempts](#).

When the specified period has elapsed, the password-based access is automatically released again for the relevant user.

A locked access can also be released again before the set time has elapsed. The administrator must in this case assign a new password in the user settings.

If you set value **0** for [LockoutTime](#), the password-based access for users is not automatically unlocked again. The administrator must in this case assign a new password in the user settings.

The set value is evaluated in milliseconds.

- **PeriodOfInactivity**

Specifies the days of inactivity before locking a user.

NOTICE: Value 0 disables this parameter

- **MinimumChangedCharacters**

Specifies how many characters must be changed at least or the passphrase.

Start the configuration

How to change the system-spanning policies for user passwords:

- 1) Open the following configuration file with a text editor:

PassphrasePolicyConfig.xml

You find this file in the following folder of the computer system set up on OpenScape UC Application.

<Osc-Install⁷³>/common/conf/

- 2) Adjust the desired settings in the following file section.

```
...
<PassphrasePolicy>
  <Type>pwd</Type>
  <MinimumAge>86400000</MinimumAge>
  <MaximumAge>777600000</MaximumAge>
  <MinimumLength>8</MinimumLength>
  <MaximumLength>0</MaximumLength>
  <MinimumDigits>1</MinimumDigits>
  <MinimumSpecialCharacters>1</MinimumSpecialCharacters>
  <MinimumUpperCaseCharacters>1</
MinimumUpperCaseCharacters>
  <MaximumRepeatedCharacters>3</
MaximumRepeatedCharacters>
  <MaximumFailedAttempts>5</MaximumFailedAttempts>
  <PasswordHistoryDepth>5</PasswordHistoryDepth>
```

⁷³ *<Osc-Install>* is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

```
<LockoutTime>1800000</LockoutTime>
<PeriodOfInactivity>90</PeriodOfInactivity>
<MinimumChangedCharacters>3</MinimumChangedCharacters>
</PassphrasePolicy>
...
```

You find a more detailed description of the single parameters in [Extract from the file PassphrasePolicyConfig.xml](#) on page 572.

- 3) Save the changes in the configuration file.
- 4) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 5) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 6) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 7) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

- 8) Look in the list for the **Logon service** component and select the check box of the component.

IMPORTANT: By the following step, the logon service will be stopped and immediately restarted without any further query. Users can therefore not log on to the OpenScape system for a moment.

- 9) Click on **Restart**.

You have now changed the system-spanning policies for user passwords and activated the modifications by a logon service reboot.

6.25.7 Changing Policies for User PINs

A user PIN must comprise eight to 16 digits by default.

Furthermore, the following applies by default:

- Each user must change his/her PIN after 90 days at the next PIN-based login.

NOTICE: This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant user settings.

- A user must not enter an incorrect PIN more than five times. If this number is exceeded, his/her user account is automatically locked for PIN-based access.

Locking the PIN-based access does not influence the password-based access of the relevant user.

- The last five PINs of a user are stored in a PIN history. A user cannot configure a PIN that is contained in his/her PIN history.

You can adjust these policies, valid for the entire system, in the following XML file:

PassphrasePolicyConfig.xml

You find this file in the following folder of the computer system set up on OpenScape UC Application.

<Osc-Install⁷⁴>/common/conf/

Extract from the file PassphrasePolicyConfig.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PassphrasePolicyConfig version="2.0">
...
<PassphrasePolicy >
  <Type>pin</Type>
  <MinimumAge>86400000</MinimumAge>
  <MaximumAge>777600000</MaximumAge>
  <MinimumLength>8</MinimumLength>
  <MaximumLength>16</MaximumLength>
  <MinimumDigits>8</MinimumDigits>
  <MinimumSpecialCharacters>0</MinimumSpecialCharacters>
  <MinimumUpperCaseCharacters>0</
MinimumUpperCaseCharacters>
  <MaximumRepeatedCharacters>0</MaximumRepeatedCharacters>
  <MaximumFailedAttempts>5</MaximumFailedAttempts>
  <PasswordHistoryDepth>5</PasswordHistoryDepth>
  <LockoutTime>1800000</LockoutTime>
  <PeriodOfInactivity>90</PeriodOfInactivity>
  <MinimumChangedCharacters>3</MinimumChangedCharacters>
</PassphrasePolicy>
```

The following parameters of this XML file control the user PIN policies valid for the entire system.

- [MinimumAge](#)
- [MaximumAge](#)
- [MinimumLength](#)
- [MaximumLength](#)
- [MinimumDigits](#)
- [MinimumSpecialCharacters](#)
- [MinimumUpperCaseCharacters](#)
- [MaximumRepeatedCharacters](#)
- [MaximumFailedAttempts](#)
- [PasswordHistoryDepth](#)
- [LockoutTime](#)
- [PeriodOfInactivity](#)
- [MinimumChangedCharacters](#)

These settings have the following functions.

⁷⁴ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

- **MinimumAge**

Specifies the period after a PIN alteration in which a user must not change his/her PIN again.

This period is only effective between two PIN modifications performed by a user himself/herself. If the administrator resets the user PIN, the relevant user can immediately change his/her PIN.

The set value is evaluated in milliseconds.

- **MaximumAge**

Specifies the period after which a user must change his/her PIN the next time he/she logs in. If you set value **0**, you disable the automatic PIN alteration prompt.

The set value is evaluated in milliseconds.

NOTICE: This system-spanning setting can be disabled for the respective user. If this is desired, activate the **Telephony PIN never expires** option on the **Password / PIN** tab of the relevant user settings.

- **MinimumLength**

Specifies the number of characters a user PIN must at least consist of.

- **MaximumLength**

Specifies the number of characters a user PIN must not exceed. If you set value **0** this policy is not used.

- **MinimumDigits**

Specifies the number of digits a user PIN must at least have.

NOTICE: On a telephone, users can only enter digits but no letters. Therefore, this setting must correspond to the setting under **MinimumLength**.

- **MinimumSpecialCharacters**

Since users can only enter digits but no letters on a telephone, this setting does not apply for PINs.

It must have value **0**.

- **MinimumUpperCaseCharacters**

Since users can only enter digits but no letters on a telephone, this setting does not apply for PINs.

It must have value **0**.

- **MaximumRepeatedCharacters**

Specifies how often a digit may successively occur in the PIN.

Example: The PIN **455587** is only valid if this parameter has at least been set to **3**. For, digit **5** appears in the PIN three times in a row.

If you set value **0** this policy is not used.

- **MaximumFailedAttempts**

Specifies how often a user may enter an incorrect PIN during the PIN-based login. If a user exceeds this number, his/her user account will automatically be locked for PIN-based access.

Locking the PIN-based access does not influence the password-based access of the relevant user.

If you set value **0** this policy is not used.

- **PasswordHistoryDepth**

Specifies how many of the last PINs are stored in the PIN history of each user. A user cannot configure a PIN that is contained in his/her PIN history.

The PIN history is administered independently from the password history.

This policy is not used when the administrator assigns a PIN to a user.

- **LockoutTime**

Specifies how long the telephone-based access is locked for a user if he/she has entered an incorrect PIN more often than is defined under [MaximumFailedAttempts](#).

When the specified period has elapsed, the telephone-based access is automatically released again for the relevant user.

A locked access can also be released again before the set time has elapsed. The administrator must in this case assign a new PIN in the user settings.

If you set value **0** for [LockoutTime](#), the telephone-based access for users is not automatically unlocked again. The administrator must in this case assign a new PIN in the user settings.

The set value is evaluated in milliseconds.

- **PeriodOfInactivity**

Specifies the days of inactivity before locking a user.

NOTICE: Value 0 disables this parameter

- **MinimumChangedCharacters**

Specifies how many characters must be changed at least or the passphrase.

Start the configuration

How to change the system-spanning policies for user PINs:

- 1) Open the following configuration file with a text editor:

PassphrasePolicyConfig.xml

You find this file in the following folder of the computer system set up on OpenScape UC Application.

<Osc-Install⁷⁵>/common/conf/

- 2) Adjust the desired settings in the following file section.

...

⁷⁵ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

```
<PassphrasePolicy>
  <Type>pin</Type>
  <MinimumAge>86400000</MinimumAge>
  <MaximumAge>777600000</MaximumAge>
  <MinimumLength>8</MinimumLength>
  <MaximumLength>16</MaximumLength>
  <MinimumDigits>8</MinimumDigits>
  ...
  <MaximumFailedAttempts>5</MaximumFailedAttempts>
  <PasswordHistoryDepth>5</PasswordHistoryDepth>
  <LockoutTime>1800000</LockoutTime>
  <PeriodOfInactivity>90</PeriodOfInactivity>
  <MinimumChangedCharacters>3</MinimumChangedCharacters>
</PassphrasePolicy>
```

You find a more detailed description of the single parameters in [Extract from the file PassphrasePolicyConfig.xml](#) on page 577.

- 3) Save the changes in the configuration file.
- 4) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 5) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 6) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 7) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 8) Look in the list for the **Logon service** component and select the check box of the component.

IMPORTANT: By the following step, the logon service will be stopped and immediately restarted without any further query. Users can therefore not log on to the OpenScape system for a moment.

- 9) Click on **Restart**.

You have now changed the system-spanning policies for user PINs and activated the modifications by a logon service reboot.

6.25.8 Synchronizing License Assignments anew

The license database of the OpenScape system may at times contain contradictory information for a profile. As a result, the license control of the

OpenScape system may withdraw privileges from users with this profile though such privileges are displayed in the profile management for the relevant profile.

In this case you can manually correct the inconsistencies in the license database.

Start the configuration

How to correct inconsistencies in the license database:

- 1) Open the profile for which you have detected inconsistencies in the license database. Change any privilege in the profile.
- 2) Save the modification.

The license database will then be newly synchronized for the relevant profile. Faulty profile assignments will then also be corrected for the relevant profile.

- 3) Cancel the modification you made in step 2.
- 4) Save the profile again.

You have now corrected the contradictory information in the license database for the relevant profile.

6.25.9 Creating a Firewall Rule in OpenScape Voice

You need to configure the connecting data of the OpenScape Voice system in the OpenScape Voice Assistant so that the OpenScape Voice Assistant can access the OpenScape Voice system.

If saving the configured settings fails in this process though the previous connection test was successful with these settings, you need to create a new firewall rule.

Start the configuration

How to create a new firewall rule via OpenScape Voice startCli:

- 1) Log on to OpenScape Voice as user **sysad**.
- 2) Start startCli.
- 3) Select 6 (**Application Level Management**).
- 4) Select 8 (**Network Element Security Management**).
- 5) Select 4 (**Packet Filter Rules Security Management**).
- 6) Select 1 (**Create**).
- 7) Create a new firewall rule with the following parameters.

• Remote FQDN:	<IP address ⁷⁶ >
• Transport Protocol:	3 (TCP)
• Remote Port Begin:	0 (All Ports)
• Direction:	1 (incoming)
• Local Host:	oam_ip_alias
• Local Port Begin:	8767

⁷⁶ IP address of the computer system on which OpenScape Voice Assistant is installed

• Local Port End:	0 (Only Local Port Begin Valid)
• Action:	1 (Allow)

8) Copy the setting.

You have now created a firewall rule that allows the OpenScape Voice Assistant to access the OpenScape Voice system.

6.25.10 Changing IP Addresses / FQDNs of the UC Application Computer Systems

NOTICE: If you change the IP address or FQDN of a UC Application computer system you need to execute the script described here only if the changed setting is also used as reference in the response file. If, for example, you change only the IP addresses of UC Application computer systems but the relevant computer systems in the response file are only referenced e. g. by FQDN, you need not execute the script described here.

You can use the following script for changing the IP addresses or FQDNs of available UC Application computer systems after the installation of OpenScape UC Application:
`changeSFwip.sh`

`[-CPFt]`

`-c <command>`

`[-i <input response file>]`

`[-o <output response file>]`

`[-n <HP8K node.cfg file>|none]`

`[-a <new ip address|host>]`

Command options:

<code>-C:</code>	Confirm modifications
<code>-P:</code>	Query new values from user
<code>-F:</code>	Enforce reconfiguration
<code>-t:</code>	Test mode; creates a response file without reconfiguring
<code><command>:</code>	<code>list</code> <code>change</code>

Default settings:

input response file:	<code>/.../servicetools/install/conf/responsefile.txt</code>

output response file:	/tmp/responsefile.txt
HP8K node.cfg file:	/log/install/changeSFWip.log

NOTICE: new ip address|host can be used with **-n none** only.

The command options you need to use depend on the deployment scenario in which OpenScape UC Application is operated.

- [Changing the IP Address / FQDN for Small Deployment](#)
- [Changing IP Addresses / FQDNs for a Deployment Scenario different from - Small Deployment](#)

6.25.10.1 Changing the IP Address / FQDN for Small Deployment

For Small Deployment you can change the IP address or FQDN of the application computer of OpenScape UC Application.

IMPORTANT: The configuration steps in this section reset the security certificates of the application computer to their installation standard. If you use certificates adjusted for an individual certificate strategy on the application computer, you need to configure and activate these individual certificates anew. Details on this are contained in [Configuring a Certificate Strategy](#).

Start the configuration

How to change the IP address or FQDN of the application computer for Small Deployment:

- 1) Stop OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad stop
```
- 2) Change the IP address or FQDN of the computer system under **YAST > Network Devices > Network Card**.
- 3) Verify that all relevant DNS servers have been updated accordingly.
- 4) Restart the application computer with the following command:

```
shutdown -r now
```
- 5) Because OpenScape UC Application reboots with the computer system, stop OpenScape UC Application again with the following command:

```
/etc/init.d/symphoniad stop
```
- 6) Open the response file of the system setup in a text editor. Check whether the computer system therein is addressed via the IP address, the host name or the FQDN.

NOTICE: In the following step, specify for *<new address>* the address format used in the response file.

- 7) Switch to the setup directory of OpenScape UC Application on the computer system of the application computer.
- 8) Execute the following command in one line:

```
servicetools/install/bin/changeSFwip.sh -c change -n none -a <new address> -CF
```

For example:

```
servicetools/install/bin/changeSFwip.sh -c change -n none -a [IPv6 address] -CF
```

Example of the case that the computer system is referenced via IP address in the response file:

```
/servicetools/install/bin/changeSFwip.sh
```

-c change

-n none

-a 172.11.0.30

-CF
- 9) Adjust in OpenScape Voice the firewall settings you performed during the OpenScape UC Application setup via startCli.
- 10) Adjust in OpenScape Voice the settings of the endpoints that belong to the OpenScape Media Server or to the voice and conference portal.
- 11) Start OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad start
```

You have now modified the IP address or FQDN of the application computer for Small Deployment.

Possibly required reconfigurations

If you used certificates adjusted for an individual certificate strategy on the application computer, you need to configure and activate these individual certificates anew. Details on this are contained in [Configuring a Certificate Strategy](#) on page 646.

If you have changed the FQDN of the application computer and configured the Single Sign-On (SSO) feature beforehand, you need to configure this feature anew. Details on this are contained in [Configuring SSO \(Single Sign-On\)](#) on page 514.

6.25.10.2 Changing IP Addresses / FQDNs for a Deployment Scenario different from Small Deployment

For a deployment scenario different from Small Deployment you can change the IP address or FQDN of the following UC Application computer systems:

- Application computer
- Front-end computer
- Media Server computer

IMPORTANT: The configuration steps in this section reset the security certificates of the computer systems to their installation standard. If you use certificates adjusted for an individual certificate strategy on the computer systems, you need to configure and activate these individual certificates anew. Details on this are contained in [Configuring a Certificate Strategy](#).

Start the configuration

How to change the IP addresses or FQDNs of the computer systems:

- 1) Execute the following steps on every computer system of OpenScape UC Application the IP address or FQDN of which you wish to change.
 - a) Stop OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad stop
```
 - b) Change the IP address or FQDN of the computer system under **YAST > Network Devices > Network Card**.
 - c) Verify that all relevant DNS servers have been updated accordingly.
 - d) Reboot the computer system with the following command:

```
shutdown -r now
```
- 2) If you have changed the IP address or FQDN of the application computer, execute the following steps on every computer system of OpenScape UC Application. Otherwise, perform such steps only on the computer system the IP address or FQDN of which you have changed.

NOTICE: In case of Very Large Deployment you need to consider only the computer systems of the relevant cluster.

IMPORTANT: If you have changed the IP address or FQDN of the application computer you need to execute the following steps on the application computer first. Subsequently, when all UC Application services on the application computer are up again, execute such steps on the other computer systems of OpenScape UC Application.

- a) Stop OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad stop
```
- b) Open the response file of the system setup in a text editor. Check whether the different computer systems therein are addressed via the IP address, the host name or the FQDN.
- c) Switch to the setup directory of OpenScape UC Application on the computer system.
- d) Execute the following command in one line:

```
servicetools/install/bin/changeSFWip.sh  
-c change  
-n none
```

-CF

You are prompted to specify the address of the application computer of OpenScape UC Application.

Example:

Please enter new value for SI_PRIMARY_NODE_HOST (uctest7 --> 10.11.254.57):

Depending on how the application computer is referenced in the response file, enter the new or unchanged IP address or the new or unchanged host name or FQDN of the application computer.

You are prompted to specify the address of the computer system on which you are executing the changeSFWip script (local computer system).

Example:

Please enter new value for SI_LOCAL_HOST (uctest7 --> 10.11.254.57):

Depending on how the local computer system is referenced in the response file, enter the new or unchanged IP address or the new or unchanged host name or FQDN of the local computer system.

You are prompted to specify the address of the computer system that hosts the OpenScape UC Application database. This is the application computer of OpenScape UC Application.

Example:

Please enter new value for SI_DB_HOST (uctest7 --> 10.11.254.57):

Depending on how the application computer is referenced in the response file, enter the new or unchanged IP address or the new or unchanged host name or FQDN of the application computer.

Start OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad start
```

- 3) If you have changed the IP address or FQDN of the application computer, adjust in OpenScape Voice the associated firewall settings you performed during the OpenScape UC Application setup via startCli.
- 4) If you have changed the IP address or FQDN of a Media Server computer system, adjust in OpenScape Voice the associated settings of the end points that belong to the OpenScape Media Server or to the voice and conference portal.

You have now changed the IP addresses or FQDNs.

Possibly required reconfigurations

If you used certificates adjusted for an individual certificate strategy, you need to configure and activate these individual certificates anew. Details on this are contained in [Configuring a Certificate Strategy](#) on page 646.

If you have changed the FQDN of the application computer and configured the Single Sign-On (SSO) feature for SOAP-based UC Application clients beforehand, you need to configure this feature anew. Details on this are contained in [Configuring SSO \(Single Sign-On\)](#) on page 514.

If you use a single front-end computer in your deployment scenario, have changed the FQDN of this computer system and configured the Single Sign-On (SSO) feature for non-SOAP-based UC Application clients beforehand, you

need to configure this feature anew. Details on this are contained in [Configuring SSO \(Single Sign-On\)](#) on page 514.

6.25.10.3 Creating both IPV4 and IPV6 compatible Servers

It is possible for a CMP server to operate with both IPv4 and IPv6 addresses.

For a dual CMP server, execute the following steps:

- 1) Run the `ifconfig` command and copy the the IPv6 address displayed under `eth0`:

```
ifconfig eth0
```

- 2) Stop OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad stop
```

- 3) Execute the following command in one line:

```
servicetools/install/bin/changeSFwip.sh -c change -n  
none -a [IPv6 address displayed under eth0] -CF
```

- 4) Start OpenScape UC Application with the following command:

```
/etc/init.d/symphoniad start
```

6.25.11 Configuring the IPv6 Support for OpenScape Media Server

The OpenScape Media Server uses an IPv4-based network infrastructure by default. How to configure the OpenScape Media Server for an IPv6-based network infrastructure describes the *OpenScape Media Server Administration Documentation* manual.

6.25.12 Configuring the HTTPS Port for CMP Access

The CMP uses port 443 for the secured HTTPS protocol by default. You can customize this default setting.

Subsequently, administrators can only log on to the CMP via HTTPS.

Start the configuration

How to change the port for the HTTPS protocol:

- 1) Open the following Property file with a text editor:

```
PortReconfiguration.properties
```

You find this file in the following folder of the computer system on which the Tomcat server is installed with the CMP.

```
<Osc-Install77>/common/conf/
```

⁷⁷ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

- 2) Search the property file for the entry with the setting **CMP_HTTPS_PORT**, and assign it the desired port number.

Example: `CMP_HTTPS_PORT = 444`

- 3) Save the changes in the Property file.
- 4) Switch to the following directory on the computer system:

`<Osc-Install77>/servicetools/install/bin/`

- 5) Execute the `installlib` script with the following command:

`./installlib.sh reconfiguration.ports`

- 6) Wait until the script has finished.
- 7) Restart the Tomcat server with the following command:

`/etc/init.d/symphoniad restart TomcatServletContainer`

From now on administrators can only log on to the CMP via HTTPS.

Example: `https://10.52.22.118:444/management/`

6.25.13 Activating HTTP Port for Framework

IMPORTANT: Activating the HTTP protocol port **4708** in the framework of OpenScape UC Application may lead to a security gap in the OpenScape system.

The protocol port **4708** for HTTP is locked in the framework of OpenScape UC Application for security reasons. The protocol port **4711** (HTTPS) should be used for the HTTP-based communication instead – e. g. for the communication between OpenScape Desktop Client and the application computer of OpenScape UC Application.

You can use the CMP to manually activate the protocol port **4708** in the framework of OpenScape UC Application.

Start the configuration

How to activate the protocol port **4708** for HTTP in the framework of OpenScape UC Application:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Search the list for components the names of which begin with **Connector**.
6) Search the found components for the one the **Uri** setting of which has the following value:

`http://<IP address>:4708`

NOTICE: In most cases you can recognize the connector

component searched for by its having stopped (). If

all connector components are started (), the protocol port **4708** for HTTP is already active in the framework of OpenScape UC Application.

- 7) Tick the check box of the relevant component.
8) Click on **Start / Stop**.

You have now manually activated the protocol port **4708** for HTTP in the framework of OpenScape UC Application.

6.25.14 Activating the anonymized Originator Address for automatic e-mails

OpenScape UC Application can automatically send e-mails to users, e. g. invitations to web conferences. The address of an individual OpenScape user is used as originator address for such e-mails by default if the reason for this e-mail is related to a direct action of this user. For example, the invitations to a web conference are thus send with the e-mail originator address of the OpenScape user who has created the relevant web conference.

Alternatively, you may wish to send automatic e-mails always with an anonymized e-mail originator address. This originator address can then be configured under **Default Sender Address** in the groupware connector.

Start the configuration

How to activate the use of anonymized e-mail originator addresses for automatic e-mails:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Search the list for the **Notification and Prompting** component and click on the associated component name.

The dialog box with the settings of the selected component opens.

- 6) Specify the **true** value under **NOTIFY_USING_NOREPLY**.

- 7) Click on **Save** to copy the settings.

- 8) In the list entry of the **Notification and Prompting** component, click  to open the action menu of the component.

IMPORTANT: By the following step, the component will be stopped and immediately restarted without any further query. This interrupts the notification services of the OpenScape system.

- 9) In the actions menu, select **Restart**.

The **Notification and Prompting** component is restarted.

From now on, automated e-mails are always sent with the anonymized default sender address.

6.25.15 Configuring Scheduled Message Routing

A message left by a caller for an OpenScape user in the voice portal's guest access is forwarded to the external groupware or voicemail system and stored in the relevant user's inbox by a UC Application workflow agent.

If the groupware or voicemail system cannot be reached when the message is forwarded, the workflow agent buffers the message and tries to forward it at a later date. The workflow agent carries out this forwarding attempt ten times in two-minute intervals by default.

If the message can still not be forwarded, it is deleted without having been forwarded.

You can configure the parameters for repeated message delivery.

Start the configuration

How to configure the parameters for repeated message delivery:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Wfa Service** component and click on the associated component name.

The dialog box with the settings of the selected component opens.

- 6) Specify in the **MessageTransferApplication.MAXRETRY** field how often the workflow agent shall try to forward a message.
- 7) Specify in the **MessageTransferApplication.RETRYINTERVAL** field how many minutes the workflow agent shall wait after a failed forwarding attempt until starting the next attempt.
- 8) Select **Save** to copy the new settings.

You have now configured the parameters for repeated message delivery.

6.25.16 Transmitting Information about OpenScape 4000 Resources to OpenScape UC Application

NOTICE: You need to execute the steps described in this section only every time you change data in the OpenScape 4000 system for OpenScape 4000 subscriber connections, dial plans, numbering plans and subscribers.

Information about OpenScape 4000 subscriber connections, dial plans and numbering plans must be transferred to OpenScape UC Application from OpenScape 4000.

If you have connected several communications systems to OpenScape UC Application directly, you need to execute the configuration steps of this chapter for each of the directly connected communications systems.

Start the configuration

How to transmit information from OpenScape 4000 to OpenScape UC Application:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

You see all nodes that are available in the OpenScape system.

- 2) Search the list for the OpenScape 4000 nodes the information of which you wish to transfer to OpenScape UC Application and click on  to open this node's action menu.
- 3) In the actions menu, select **Synchronize Versions**.
A window opens that displays the synchronization progress and end.
You have now transferred the required information from OpenScape 4000 to OpenScape UC Application.

6.25.17 Activating the Call Acceptance for remote preferred Devices

A user can select any device in an OpenScape client as the preferred device. For accepting calls in an OpenScape client however, this device must be set as an associated/assigned device on the user, otherwise the answer button will be hidden.

In order to deactivate this feature and allow a user to answer a call on any preferred device follow the steps below:

- 1) Open a shell on the application computer.
- 2) Switch to the following directory:
`<Osc-Install78>/common/conf/config-beans`
- 3) Execute the following command in the shell:
`grep MASK_ANSWERCALL instance*`
The name of the instance file to be changed is displayed.
- 4) Open the relevant file with a text editor.
- 5) In this file, change the value for the **MASK_ANSWERCALL** parameter from **ON** to **OFF**.
- 6) Save the changes in the file.
- 7) Execute the following command to restart system and see the changes:
`/etc/init.d/symphoniad restart`

6.25.18 Managing Network Address (NAT) Translations

To hide the structure of the UC Application network to the outside you can use NAT mapping tables with OpenScape UC Application. Such NAT mapping tables ensure that for SOAP- and HTTP-based communication of OpenScape Desktop Client or OpenScape Mobile Client only addresses that can be decoupled from the network infrastructure are published and not the hardware-based addresses of the UC Application systems.

NAT mapping tables are part of the system file `system.xml`, which is available on every computer system of OpenScape UC Application and contains basic infrastructure information of the UC Application system. The system file `system.xml` is newly loaded from the application computer after every start

⁷⁸ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

of a UC Application computer system, thus being synchronized between the different computer systems of a UC Application system.

You find the `system.xml` file in the following directory of a UC Application computer system:

```
<Osc-Install79>/common/conf/
```

6.25.18.1 Structure of an NAT Mapping Table

In the `system.xml` file you can add an NAT mapping table to every UC Application node. It has the following basic format:

```
<Node displayname="Backend" guid="72ababd8-e065-4ba5-
b5b1-c8ed32ccf5b0" host="athol60" jGroupsPort="7800"
serviceContainer="true" type="BACKEND">
  <NATMappingTable>
    <Entry hostExternal="openscapebe.company.com"
tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
```

`hostExternal` defines the fully qualified domain name to be used for the relevant UC Application node instead of the hardware-based addresses.

`tenantID` defines a reference ID in the system used for referencing an individual NAT entry in a mapping table.

You can theoretically configure several entries with different values for `tenantID` in every NAT mapping table. One for all OpenScape Mobile Clients used and one for all OpenScape Desktop Clients used. However, it is sufficient to use one mapping entry for both client types.

Simplified mapping example of OpenScape Desktop Client

While the OpenScape Desktop Client is setting up the communication to the UC Application system, it transfers the address entered in its configuration under **OpenScape Web Client host address** to OpenScape UC Application. This address is compared with the values of `tenantID` in the NAT mapping table for every UC Application computer system.

If e. g. the following NAT mapping table is configured for the application computer in a UC Application system and the transferred address from **OpenScape Web Client host address** corresponds to value **openscape.company.com**, the address **openscapebe.company.com** is transferred to the relevant OpenScape Desktop Client for communicating with the application computer.

```
<Node displayname="Backend" guid="72ababd8-e065-4ba5-
b5b1-c8ed32ccf5b0" host="athol60" jGroupsPort="7800"
serviceContainer="true" type="BACKEND">
  <NATMappingTable>
    <Entry hostExternal="openscapebe.company.com"
tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
```

⁷⁹ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

```
</NATMappingTable>
</Node>
```

If no table entry with corresponding tenantID can be found, the hardware-based address of the relevant UC Application system is returned to the OpenScape Mobile Client.

Simplified mapping example of OpenScape Mobile Client

While the OpenScape Mobile Client is setting up the communication to the UC Application system via the Facade server, the Facade server transfers the address entered in its property file under **serverName** to OpenScape UC Application. This address is compared with the values of tenantID in the NAT mapping table for every UC Application computer system.

If e. g. the following NAT mapping table is configured for the application computer in a UC Application system and the transferred address from **serverName** corresponds to value **openscape.company.com**, the address **openscapebe.company.com** is transferred to the relevant OpenScape Mobile Client for communicating with the application computer.

```
<Node displayname="Backend" guid="72ababd8-e065-4ba5-
b5b1-c8ed32ccf5b0" host="athol60" jGroupsPort="7800"
serviceContainer="true" type="BACKEND">
  <NATMappingTable>
    <Entry hostExternal="openscapebe.company.com"
tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
```

If no table entry with corresponding tenantID can be found, the hardware-based address of the relevant UC Application system is returned to the OpenScape Mobile Client.

6.25.18.2 Configuring Network Address (NAT) Translations

You need to configure different components of the UC Application system for activating the translation of network addresses (NAT). Such components are:

- The DNS configuration of the network
- The system file `system.xml` of the application computer
- If you use the OpenScape Desktop Client, the OpenScape Desktop Client
- If you use the OpenScape Mobile Client, the Facade server

Start the configuration

How to configure the translation of network addresses:

- 1) To resolve IP addresses, adjust the DNS configuration is such a way that each OpenScape UC Application computer system can be reached under a fully qualified domain name.

Example of an application computer with two front-end and two Media Server computer systems:

openscapebe.company.com	10.4.255.212
openscapefe1.company.com	10.4.252.161

openscapefe2.company.com	10.4.252.165
openscapems1.company.com	10.4.252.20
openscapems2.company.com	10.4.252.37

- 2) If you use several frontend computers with one load balancer, add in the DNS configuration another entry for the fully qualified domain name under which the virtual server shall be reachable for the pool of all configured frontend computers. See also [Configuring the Load Balancer for Front-End Computers](#) on page 98.

Example:

openscape.company.com	10.4.255.211

- 3) Open the following file in a text editor on the application computer.

`<Osc-Install80>/common/conf/system.xml`

- 4) Add an NAT mapping entry of the following format for each UC Application node.

```
<NATMappingTable>
  <Entry hostExternal ="< FQDN of the relevant node >"
    tenantID ="< FQDN of the front-end computer pool >"/>
</NATMappingTable>
```

In doing so, use:

- The node-individual fully qualified domain name you configured in step 1 for the hostExternal parameter
- The following fully qualified domain name for all parameters tenantID
 - The fully qualified domain name you configured in step 2 if you use several frontend computers with one load balancer
 - Otherwise the fully qualified domain name you configured in step 1 for the application computer

Example of an application computer with two front-end and two Media Server computer systems:

```
<Node displayname="Backend" guid="72ababd8-e065-4ba5-b5b1-c8ed32ccf5b0" host="athol60" jGroupsPort="7800"
  serviceContainer="true" type="BACKEND">
  <NATMappingTable>
    <Entry hostExternal="openscapebe.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
<Node displayname="FE Server 1" guid="59aac72a-fedf-4977-9a57-9afd7957bf45" host="athol61"
  jGroupsPort="7800" serviceContainer="true"
  type="FRONTEND">
  <NATMappingTable>
    <Entry hostExternal="openscapefe1.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
```

⁸⁰ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

```

    </NATMappingTable>
</Node>
<Node displayname="FE Server 2"
  guid="5f92643f-7cda-43b1-a64b-5e0e87f7d502"
  host="atho165" jGroupsPort="7800"
  serviceContainer="true" type="FRONTEND">
  <NATMappingTable>
    <Entry hostExternal="openscapefe2.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
<Node displayname="MS 1"
  guid="2f2105fe-3aa4-410d-9bd9-0dcb6a1c0a26"
  host="atho37" jGroupsPort="7800"
  serviceContainer="true" type="MEDIASERVER">
  <NATMappingTable>
    <Entry hostExternal="openscapems1.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>
<Node displayname="MS 2"
  guid="d4ecaa73-8a78-4f3c-9262-783c666faa8a"
  host="atho20" jGroupsPort="7800"
  serviceContainer="true" type="MEDIASERVER">
  <NATMappingTable>
    <Entry hostExternal="openscapems2.company.com"
      tenantID="openscape.company.com"/>
  </NATMappingTable>
</Node>

```

- 5) Reboot all OpenScape UC Application computer systems so that the system.xml file is replicated on all computer systems.
- 6) Configure the following address in the OpenScape Desktop Client under **OpenScape Web Client host address**.
 - The fully qualified domain name you configured in step 2 if you use several frontend computers with one load balancer
 - Otherwise the fully qualified domain name you configured in step 1 for the application computer

How to configure **OpenScape Web Client host address** in the OpenScape Desktop Client describes the *OpenScape UC Application, OpenScape Desktop Client, Installation and Administration* manual.

- 7) Configure in the property file properties.ini of the Facade server the fully qualified host name for the serverName setting.
 - The fully qualified domain name you configured in step 2 if you use several frontend computers with one load balancer
 - Otherwise the fully qualified domain name you configured in step 1 for the application computer

The property file of the Facade server is detailed in [Managing the Facade Server](#) on page 501.

6.25.19 Suppressing Features for managing preferred Devices in the Clients

Depending on the situation, configuring more than one preferred device for a user is not reasonable. This is in particular the case if the ONS device of a user does not support forwarding via the one-number service.

To prevent users from configuring additional preferred devices, you can suppress the features for managing preferred devices user-individually in the OpenScape clients. You control suppressing the managing features via the **Disable Device List Management via Client** privilege in the OpenScape UC Application user profiles.

In the most simple case you need to create a new UC Application user profile to which the **Disable Device List Management via Client** privilege is assigned. This new user profile must then be assigned to the users for whom the features for managing preferred devices shall be suppressed.

Suppressing the management features results in the following:

- The user cannot add/remove a device to/from the list of preferred devices.
- The user can:
 - Change the device name and the ring time of preferred devices.
 - Manage named device lists and, in doing so, use the configured preferred devices.
 - Forward incoming calls by call forwarding or rules.

NOTICE: If forwardings are to be suppressed via rule management too, the **Rule** privilege must be disabled for the relevant user in addition.

Start the configuration

Create a new UC Application user profile and assign it to the relevant users by executing the following steps:

- 1) Create a new user profile. Proceed in principle as described in [Creating a User Profile](#).
 - Specify an expressive name such as **Disable Device List Management** under **Name**.
 - Select the **OpenScape UC App** option under **Application**.
 - Select exclusively the privilege **Disable Device List Management via Client**.

- 2) Assign the new user profile to the users for whom the features for managing preferred devices shall be suppressed. To this, perform the following steps:

- a) On the **Configuration** navigation tab of the click on the **Unified Communications** navigation menu item.

- b) In the navigation tree, click on **Accounts > List**.

A list of all UC Application user accounts configured in the selected domain appears in the workspace.

- c) Click on the login name of a user account for the user of which the features for managing preferred devices shall be suppressed.

The dialog with the settings of the relevant UC Application user account opens.

- d) Switch to the **Profiles** tab.

- e) Select the newly created user profile under **Assigned to user**.

- f) Select **Save**.

- g) If required, assign the newly created user profile to other users in the same manner.

From now on, managing preferred devices is restricted for the relevant user in the OpenScape clients.

6.25.20 Starting all Conferences as Video Conference

IMPORTANT: Do not perform the configuration described here if pure audio conferences are used besides video conferences in a productive system. Otherwise, video licenses and system resources would be allocated of no avail, which may restrict the system performance from the user's view.

You can configure the conference portal to have all associated conferences started as video conference across the system. In other words, a video line (m-line) is started for all connections with dialed-in conference participants; no matter whether or not the associated device supports video.

Start the configuration

How to configure the conference portal for systemwide video conferences by executing the following steps in the CMP:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.

- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or stopped .

- 5) Search the list for the **Conferencing Service** component and click on the associated component name.

The window with the conference service settings opens.

- 6) Enter value **true** in the **forceVideoConferences** field.
- 7) Leave all other conference service settings unchanged and click on **Save** to copy the settings.

All conference portal conferences will now automatically be started as video conference.

6.25.21 Copying an OpenScape Voice Resource with changed Subscriber Type

If the subscriber type of an OpenScape Voice subscriber changes from private to public or vice versa, this alteration cannot be directly copied to the OpenScape Voice resources of OpenScape UC Application. Instead, the existing OpenScape Voice resource of the relevant OpenScape Voice subscriber must first be deleted from the UC Application configuration. Then, with the next synchronization, the changed OpenScape Voice subscriber is transferred with his/her new subscriber type to OpenScape UC Application.

Start the configuration

Update an OpenScape Voice resource with changed subscriber type in OpenScape UC Application by executing the following steps in the CMP:

- 1) Select the domain the user accounts of which are later to be contained in the import file from the **Domain** selection list of the CMP system bar.

NOTICE: OpenScape UC Application can currently be operated with only one domain – the predefined system domain **system**.

- 2) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 3) Click on **Import & Export > Export** in the navigation tree.

The dialog for exporting configurations opens.

- 4) Select the check box of the **Domain Management** component under - **Common Management Platform**.
- 5) Click on **Next**.
- 6) Click on **Export**.

The selected data is loaded to the client PC as Zip file.

- 7) Store the file locally on the computer system.

- 8) Open the downloaded Zip file and open the following Zip file contained therein:

```
${exportWorkingDir}\  
Package_domainmanagement_domainmanagement001.zip
```

- 9) In there open the following file with a text editor:

```
${BackupAppWorkDir}\domain_configuration.csv
```

NOTICE: If the data is to contain special characters, you need to use a text editor that supports the UTF-8 file format. Microsoft Windows Wordpad and Microsoft Word do not support the UTF-8 file format. Notepad does.

NOTICE: The text editor used must not deploy a Byte-Order-Mark – BOM.

The exported OpenScape UC Application domain information is displayed. The data is structured as follows.

- You find the information about the OpenScape Voice resource under the entry that begins with ##Phone.
 - The fields of an entry are separated from each other by semicolon.
- 10) Find in the exported `domain_configuration.csv` file the Phone entries of the OpenScape Voice subscribers for whom the subscriber type has changed. Prefix such entries with `d :`.

This supplement has the respective resource removed from the UC Application configuration after the import. You find details about this function in the *Common Management Platform, Administrator Documentation* manual.

- 11) Save the supplemented file `domain_configuration.csv` in the CSV format.
- 12) Overwrite the original file version in the Zip file with the modified file `domain_configuration.csv`.
- 13) Click on the **Recovery** menu item on the **Maintenance** navigation tab of the CMP.
- 14) Click on **Import & Export > Import** in the navigation tree.

The dialog for importing a configuration opens.

- 15) Specify the name of the just changed zip-file in the **Import file** field. Enter the name and path or use the **Browse** button to select the file.
- 16) Click on **Next**.
- 17) Select under **Type of file to be imported** the **Common Management Platform** entry.
- 18) Select under **Included type of data** the **Domain Management** entry.
- 19) Click on **Import**.

The selected data is imported. The progress of the import procedure is displayed with a progress bar.

- 20) Check whether the relevant OpenScape Voice resources were removed from the UC Application configuration.

During the next synchronization the changed OpenScape Voice resources are transmitted to OpenScape UC Application with their new subscriber type.

- 21) Once the OpenScape Voice resources with their new subscriber type have been transferred to OpenScape UC Application, reassign them to the relevant UC Application users.

6.25.22 Configuring the Status Monitoring for OpenScape Voice Multiline Hunt Groups (MLHG)

Calls are often to be transferred to the subscribers of an OpenScape Voice multiline hunt group. In this case the availability status of the multiline hunt group can be determined from the availability status of the single multiline hunt group subscribers. This will indicate to a UC Application user whether a multiline hunt group subscriber is ready to take a call before it is transferred.

Determining the availability status of a multiline hunt group does not only consider the associated subscribers' readiness to take calls. Other hunt group events are also involved – for example:

- Agent not ready
- Agent working after call

In order to use status monitoring for OpenScape Voice multi-line hunt groups (MLHG), the “**All members busy**” notification option must have been activated in OpenScape Voice.

NOTICE: Status monitoring for OpenScape Voice multi-line hunt groups (MLHG) does not work for non-hunt DN's of OpenScape Voice. It does not work for application-controlled hunting of OpenScape Voice.

NOTICE: You find further details on monitoring the status of OpenScape Voice multiline hunt groups in the *OpenScape Voice, Administrator Documentation* manual.

Start the configuration

How to activate the status monitoring for an OpenScape Voice multiline hunt group:

- 1) Create a new UC Application user.
 - a) In doing so, assign this UC Application user a name that points to the group character of the multiline hunt group.

Example: Service Group
 - b) Assign the UC Application user the pilot phone number of the multiline hunt group as ONS number.

- 2) Activate the automatic presence monitoring approval for the UC Application user as follows:

- a) In the OpenScape Web Client for example, log on under the account of the UC Application user.

Configure: **General settings > Presence > Access Control List > If other users would like to see your presence status > provide access**

NOTICE: Alternatively, you can activate the automatic presence monitoring using the following database commands. Enter the two database commands without the given word wraps.

```
/opt/siemens/solid/bin/solsql
-e "insert into
  opensoa.sympresence.symaclpreferences
  values
  ( '<ID of the UC Application user>' ,1) "
\
-a "tcp localhost 16760" dba <database
  password>
```

```
/opt/siemens/solid/bin/solsql
-e "update
  opensoa.sympresence.symaclpreferences set
  PREFERENCE=1
where \PRESENTITYID= '<ID of the UC
  Application user>' "
-a "tcp localhost 16760" dba <database
  password>
```

From now on, regular UC Application users may monitor the availability status of the multiline hunt group by monitoring the presence status of the just created UC Application user.

6.25.23 Restricting the Visibility of Contacts based on Groups

OpenScape UC Application provides various connectors for finding contacts in different directories. Such connectors comprise for example the connector for connecting an external LDAP directory or the connector for connecting system-wide user directories.

Finding contacts using those connectors can be deployed for the following applications:

- UC Application users can determine the contact data of other users via contact search.
- Intrasystem services use the contact search to resolve user names and phone numbers against each other – for example to display names in the call journal.

In the contact search scope you can restrict the visibility of contacts as follows:

- Each contact search connector can be made available exclusively to UC Application users who belong to an individual user group – a so-called visibility group.

- UC Application users may belong to none or any number of visibility groups.
- If UC Application users have access to selected contact search connectors only, the following applies:
 - Users may deploy only those selected connectors for finding contact data.
 - UC Application services may use only those selected connectors to resolve user names and phone numbers against each other for the relevant users.

NOTICE: Restricting the visibility of contacts requires a project-specific release. You can obtain details of such a solution from Professional Services & Solutions (PS & S) of Unify Software and Solutions GmbH & Co. KG.

6.25.24 Changing the Service Account for UC Application Services

The OpenScape UC Application services are started and executed under the root service account by default.

However, security reasons may deem it useful to change this behavior in that only the start script of OpenScape UC Application is launched under the root service account. The start script then launches the required UC Application services under the sym service account. As a result, the OpenScape UC Application services have only restricted system privileges.

NOTICE: Selected UC Application services still require root privileges. Such services are specified in the `/etc/sudoers` file.

IMPORTANT: In order to be able to restore the system in case of an error, be sure to have a backup for the UC Application computer systems. This applies for the application computer and all front-end and Media Server computers that may be available.

Start the configuration

Change the service account for the OpenScape UC Application services from root to sym by executing the following steps:

- 1) Check that the following packages were installed on the application computer during the installation of OpenScape UC Application:
 - `libcap-progs` (from the SLES installation data carrier)
 - `deroot-scripts` (from the UC Application installation data carrier)

If these packages have not been installed yet, install them now.

- 2) Open the following file on the OpenScape UC Application application computer:

`/boot/grub/menu.lst`

- 3) Attach the following expression to the end of each kernel start option:

`file_caps=1`

Example of a kernel start option: `kernel /vmlinuz-3.0.13-0.27-default root=/dev/OpenScapeUC/UC1 resume=/dev/sda2 splash=silent crashkernel=256M-:128M showopts vga=0x314 file_caps=1`

- 4) Reboot the operating system of the application computer.
5) Open a shell as root on the application computer and execute the following script:

`<Osc-Install81>/servicetools/deroot/deroot.sh`

- 6) If you use a deployment scenario with front-end and Media Server computers, execute the described steps on these computer systems also.

The OpenScape UC Application services now operate under the sym service account.

NOTICE: If this setting proves problem-ridden, you can undo changing the service account. Execute the following script in the above described manner on the previously reconfigured computer systems: `<Osc-Install>/servicetools/deroot/rollback.sh`

6.26 Managing OpenScape Outlook Extensions

This OpenScape Extensions V1R5 for Microsoft Outlook replaces the SOAP interface by the WebSocket interface as the way to communicate with OSC UC Applications Server.

The new WebSocket interface offers the possibility to use OpenScape Extensions V1R5 in the internet without the need to have a VPN connection in place to connect to OpenScape UC Applications Server.

WebSocket connection uses the ports 7789 (non secure) and 8443 (secure).

As it's replaced, the SOAP connection to OpenScape UC Applications Server is not supported in this version.

The update from previous OL Extensions V1.0 to V1.5 can be performed normally. The used SOAP ports (4708/non secure, 4709/secure) are automatically replaced during the update by the corresponding WebSocket interface ports (7789/non secure, 8443/secure).

6.27 Configuring WebRTC support to OSV failover

SIP gateway must ensure that in case of an OSV cluster failover the traffic for/to WebRTC lines will be redirected to the standby OSV node.

This is feasible via a DNS-srv FQDN support where a DNS lookup is performed to identify the SIP registrar/server address and redirect connection of back to

⁸¹ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

back SIPUA of the SIP service provider to the SIP signaling manager of the active OSV node.

Please execute the following steps in order to properly configure the UC/OSV environment to have the redundancy for WebRTC lines.

6.27.1 DNS SRV Configuration

In order to configure WebRTC redundancy, a DNS SRV configuration is required in a DNS server.

To create SRV record:

- 1) Open the DNS manager and create new zone by right-clicking on Forward lookup zones to open the New Zone Wizard. Click Next.
- 2) In the Zone Type window, select Primary Zone and click Next.
- 3) In the Active Directory Zone Replication Scope window, select the option To all domain controllers in this domain.. and click Next.
- 4) Enter a name under Zone name field of the Zone Name window and click Next.

e.g. grp1019.node1.lab

- 5) In the Dynamic Update window, select the option Allow only secure dynamic updates and click Next.
- 6) In the Completing the New Zone Wizard window, click Finish to complete the new zone creation.
- 7) Now, locate the new zone (e.g. grp1019.node1.lab) right click and select other record.
- 8) Select service location (SRV) and Click Create Record..
- 9) In the New Resource Record window that follows, enter the following values in the parameter fields:

- Service: _sip
- Protocol: _tcp
- Priority: 0 (Is the priority for node1)
- Weight: 0
- Port number: 5060
- Host offering this service: grp1019sipsm1vip.h8k.sec (Is the FQDN of node1)

Click OK.

- 10) Again right click and select other record.
- 11) Select service location (SRV) and Click Create Record..

- 12) In the New Resource Record window that follows, enter the following values in the parameter fields:

- Service: `_sip`
- Protocol: `_tcp`
- Priority: 1 (Is the priority for node2)
- Weight: 0
- Port number: 5060
- Host offering this service: `grp1019sipsm2vip2.h8k.sec` (Is the FQDN of node2)

Click OK.

IMPORTANT: Host offerings in both nodes should be created in the `h8k.sec` domain as an FQDNs that would belong to the `sipsm` of the node1 and node2.

6.27.2 UC-OSV Configuration

- 1) Open BE UC and via SSH navigate to: `path/opt/siemens/HiPathCA/config/common`
- 2) With VI edit the `WebClientServlet.cfg` as below:

```
ContactMerge_firstNameNotEqual = -0.1
ContactMerge_lastNameNotEqual = -0.1
ContactMerge_phoneNotEqual = 0
ContactMerge_emailNotEqual = 0
ContactMerge_imNotEqual = -0.2
ContactMerge_presenceNotEqual = -0.2
ContactMerge_companyNotEqual = -0.1
ContactMerge_departmentNotEqual = -0.1
ContactMerge_availabilityNotEqual = -0.3

# List of presence states shown to the user
# restricts the presence states available to user to the configured ones
# Possible values and presence states:
# active -> AVAILABLE
# away -> AWAY
# outofservice -> BE RIGHT BACK
# busy -> BUSY
# doNotDisturb -> DO NOT DISTURB
# meeting -> IN MEETING
# e.g. AvailablePresenceStates = active, away, busy

AvailablePresenceStates =

# Hier Conferencing to run in restricted mode. This means that some operations will be accessible only by the involved parts (participants/ creator) and not by any other external entity.
# This option will disable (for security purposes) functionalities such as adding a conference on behalf of another user.
# AvailablePresenceStatesRestrictedMode = false

# Set the SameSite property for the OpenScapeUC cookie. Possible values: Lax, Strict and None. None is the default value.
OpenScapeUC_SameSite = None

# Set the option to persist the state of OpenScapeUC cookie. This means that the state of the cookie will be held on server side and it will be possible to revoke it making it impossible to
# be used again by anyone. the default value is false.
OpenScapeUC_PersistState = false

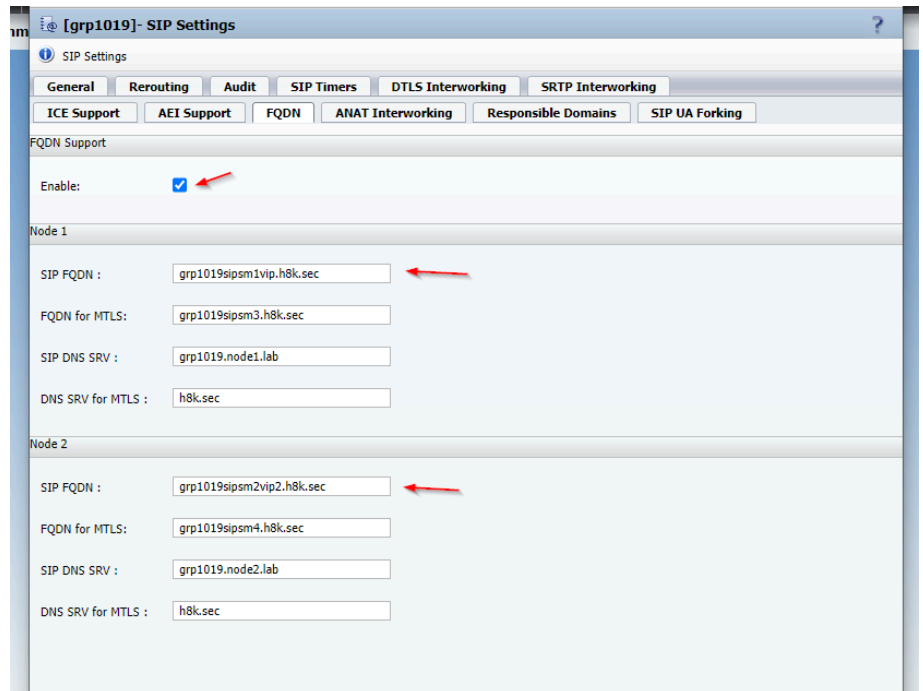
# Specify the NotificationMiddleware URL. Default value is empty.
NotificationMiddleware_URL =
NotificationMiddleware_username =
NotificationMiddleware_password =
NotificationMiddleware_certificate_location =

# Specify the SIP DNS SRV FQDN that will be used for WebRTC registration instead of the SIP IP. Default value is empty which means that SIP IP is used.
SipDnsSrvFqdn = sip1019.node1.lab

WebClientServlet.cfg lines 33-77/77 (60%)
```

- 3) In the bottom of the file locate `SipDnsSrvFqdn` and fill in the SRV created.
e.g. `grp1019.node1.lab`
- 4) Save file.
- 5) Restart the `WebClient` service to apply changes.
- 6) Now open CMP and navigate to Administration > Signaling > SIP.

- 7) In the SIP Settings window and verify that SIP FQDN in both nodes are the same as in the DNS SRV section, as show in the figure below:



6.28 OSMO Configuration via QR Code

A QR code image can be displayed in the WebClient user profile to allow the configuration of the user's OSMO client. The QR code contains the UC server URL, UC user name and the mobile number. The users can scan the QR code with their devices and the required data will be retrieved in the account details of the OSMO application. This method simplifies the OpenScape Mobile boarding procedure and avoids typing errors.

The user password will not be provided through QR codes. The user will be required to enter manually the password credentials after successfully scanning the QR code.

Two parameters are offered in the WebClientUI.cfg file for the activation of this feature:

- Enable/disable the creation of the QR code Tab View.
- Set the server URL used to login with OpenScape Mobile.

If this parameter is empty, the WebClient will use the navigation URL as the server URL.

```
#
# The "QR Code" tab allows the user to see the QR Code with informations to configure the OpenScape Mobile.
# If set to true, the profile.allowOpenScapeMobileQRcodeTabView variable enables the "QR Code" tab in the profile.
# One of the parameters presented in the QR code is the server url used to login with OpenScape Mobile.
# The profile.openScapeMobileQRcodeServerUrl variable sets the server url that will be used in the QR Code.
# If the profile.openScapeMobileQRcodeServerUrl it's empty, the WebClient will use the navigation url.
#
profile.allowOpenScapeMobileQRcodeTabView = false
profile.openScapeMobileQRcodeServerUrl =
```

7 System Monitoring

This chapter provides information about the following topics:

- [Logging OpenScape UC Application](#)
- [Logging OpenScape Voice](#)
- [Logging the SIP Traffic between OpenScape Voice and a Device](#)
- [Logging OpenScape 4000](#)
- [Logging the Groupware Service](#)
- [Logging the Web Server Component](#)
- [Logging the OpenScape Desktop Integration Tool](#)
- [Logging Nuance Vocalizer \(TTS\)](#)
- [Compression of Log-files for WebClient](#)

Manual *OpenScape Common Management Platform, Configuration and Administration* provides general information on the system logging in the CMP.

7.1 Logging OpenScape UC Application

This chapter provides information about the following topics:

- [Checking the System Components' Start](#)
- [Activating the Conferencing Component Logging](#)
- [Activating the Domain Component Logging](#)
- [Collecting Log and Dump Information automatically](#)
- [Putting out Software Versions of the UC Application Components \(productInventory.sh\)](#)

7.1.1 Checking the System Components' Start

The *uctest* application is delivered with OpenScape UC Application. You can use this application to determine whether all UC Application services have booted successfully and OpenScape UC Application is operable.

In order to find whether the UC Application services have been started, *uctest* looks for

- The *Monitoring is probably complete* message in the `osgi.log` log file and
- A considerably decreasing number of log messages in the OpenScape Web Client logging as striking system features.

Furthermore, *uctest* performs the following tests to check whether the UC Application services are available:

- OpenScape Web Client availability by means of the Apache HTTP client.
- CMP access availability by means of the Apache HTTP client.
- Availability of the SIP port on all computer systems on which the OpenScape Media Server is installed.
- Receiving a presence change event if a click-to-dial action is performed by employing a test user.

You find the *uctest* application in the following directory.

<Osc-Install⁸²>/servicetools/uctest/

Invocation and parameters of *uctest*

You can invoke the *uctest* application in the following notations:

- `uctest.sh [-d] [-t] [-w] user=<user> userpassword=<user password> admin=<administrator> adminpassword=<admin password> number=<telephone number> [sipPort=<sip tcp port>] [webClientPort=<web client https port>]`
- `uctest.sh [-d] [-t] [-w] -p`
- `uctest.sh [-d] [-t] [-w] -c <configFile>`

The parameters have the following meaning:

parameter	Meaning
-D	Activates debug messages of <i>uctest</i> put out via the default output (stdout).
-t:	Activates monitoring the log messages in the OpenScape Web Client logging.
-w	Activates the waiting option. If one of the following availability tests fails, <i>uctest</i> will start a check loop after 30 seconds in which all availability tests will be repeated until the system is available according to the tests: • Search for the <i>Monitoring is probably complete</i> message in the <code>osgi.log</code> log file. • If the -t parameter is used: Monitoring of the log messages in the OpenScape Web Client logging.
User	User account deployed for the OpenScape Web Client availability test. You must specify the account in domain notation. NOTE: In OpenScape UC Application, a directory number must have been assigned to the specified user account.
userpassword	Password for the user account under user.
admin	Administrator account used for the CMP availability test. You must specify the account in domain notation.
adminpassword	Password for the administrator account under admin.

⁸² <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

parameter	Meaning
number	Directory number used for the click-to-dial action. NOTE: You must not use the directory number assigned to the user account under user here.
sipPort	SIP port used for the OpenScape Media Server availability test. If no SIP port is specified, <i>uctest</i> will use port 5060.
webClientPort	HTTPS port used for the OpenScape Web Client availability test. If no HTTPS port is specified, <i>uctest</i> will use port 8443.
-p	Activates the interactive query for the following parameters: • User • userpassword • admin • adminpassword • number • sipPort • webClientPort
-C	References a configuration file that contains all parameters required for invoking the application. The configuration file structure demands: • Each parameter must stand in an individual line. • The value of each parameter must be enclosed in single quotation marks ('). Example: <pre>user='user.12055@system' userpassword='Open5cape!' admin='Administrator@system>' adminpassword='Open5cape!' number='12055' sipPort='5061'</pre> NOTE: To avoid unauthorized reading of passwords, only user root may receive read privileges for the configuration file.

Example 1: Operable system

```
./uctest.sh -w -t user=user.12050@system
userpassword='01*Test!' adminpassword='Asd123!..' admin
='Administrator@system' number=12055
Ok, BCOM monitoring finished at: 2014-6-2 10:49:3
Startup complete looks good at: 2014-6-2 10:49:33 (Trace
lines: 1 Maximum: 61)
Login to Web Client on vmlargefel.h8k.sec successful!
Login to Web Client on vmlargefe3.h8k.sec successful!
Login to Web Client on vmlargefe2.h8k.sec successful!
Test Media Server: vmlargems1.h8k.sec ok
Test Media Server: vmlargems3.h8k.sec ok
Test Media Server: vmlargems2.h8k.sec ok
Logon to CMP on vmlargebel.h8k.sec successful!
Device media presence change test successful!
Test CPU: idle rate: 99.3% >= 90%: ok
```

Summary: All tests are successful!

Example 2: System not ready for operation

```
./uctest.sh -w -t user=user.12050@system
userpassword='01*Test!' adminpassword=Asd123!..'
admin='Administrator@system' number=12055
Ok, BCOM monitoring finished at: 2014-6-2 10:49:3
Startup complete looks good at: 2014-6-2 10:49:33 (Trace
lines: 1 Maximum: 61)
Login to Web Client on vmlargefel.h8k.sec successful!
Login to Web Client on vmlargefe3.h8k.sec successful!
Login to Web Client on vmlargefe2.h8k.sec successful!
Test Media Server: vmlargems1.h8k.sec ok
Test Media Server: vmlargems3.h8k.sec ok
Test Media Server: vmlargems2.h8k.sec ok
Logon to CMP on vmlargebel.h8k.sec successful!
Login to Web Client on vmlargefel.h8k.sec failed!
Check user (user.12050@system) and password!
Device media presence change test failed!
Test CPU: idle rate: 99.3% >= 90%: ok
```

7.1.2 Activating the Conferencing Component Logging

IMPORTANT: Logging the Conferencing component may allocate a considerable amount of computing performance of the UC Application system. This may deteriorate the system performance from the point of view of the user. Therefore, activate the logging only for the time required to search for an error.

To analyze errors of the Conferencing component you must activate logging this component. The data logged in such a way helps to analyze and rectify product errors faster.

The collected logging data is stored in the Symphonia log. You find the associated log files under:

/var/siemens/common/log/symphonia

How to activate logging the Conferencing component:

- 1) Click on the **Monitoring** menu item on the **Maintenance** navigation tab of the CMP.

- 2) Click in the navigation tree on **Tools & Utilities > Configuration Files**.

A list of all system nodes is displayed in the work area. Under **Active File** you can see for each of these nodes which configuration file is currently active for logging.

- 3) Execute the following steps for the application computer and for each Media Server node of your UC Application environment:

- a) Note down the configuration file currently active for the node (**Active File**).

You will need this information to reactivate the original configuration file at a later date.

- b) Click on the name of the respective node.

The window that contains the available configuration files opens.

- c) Click in the list entry of the `log4j_conferencing.xml` configuration

file on  to open the associated action menu.

- d) In the actions menu, select **Activate...**

The window for activating the configuration file opens.

- e) Enter your name under **Name**.

This information is logged for later research.

- f) Specify under **Reason for Activation** why you change the logging configuration of the node.

This information is logged for later research.

The window for activating the configuration file closes.

The list of system nodes displays the newly activated configuration file for the respective node under **Active File**.

- g) Click in the list entry of the respective node on  to open the associated action menu.

- h) In the actions menu, select **Start new Log File**.

Logging the Conferencing component in a new log file thus begins.

- i) Execute these steps for the application computer and for each Media Server node of your UC Application environment.

After you have finished reenacting a problem, reactivate for each system node the configuration file that was active before you switched to the conferencing logging.

Proceed as described for the `log4j_conferencing.xml` configuration file.

NOTICE: You cannot activate the `default_log4j.xml` configuration file in this way. Instead, activate this configuration file by means of **Activate default configuration** in the action menu of the relevant system node.

7.1.3 Activating the Domain Component Logging

IMPORTANT: Logging the Domain component may allocate a considerable amount of computing performance of the UC Application system. This may deteriorate the system performance from the point of view of the user. Therefore, activate the logging only for the time required to search for an error.

To analyze errors of the Domain component you must activate logging this component. The data logged in such a way helps to analyze and rectify product errors faster.

The collected logging data is stored in the Symphonia log. You find the associated log files under:

`/var/siemens/common/log/symphonia`

How to activate logging the Domain component:

- 1) Click on the **Monitoring** menu item on the **Maintenance** navigation tab of the CMP.
- 2) Click in the navigation tree on **Tools & Utilities > Configuration Files**.

A list of all system nodes is displayed in the work area. Under **Active File** you can see for each of these nodes which configuration file is currently active for logging.

3) Execute the following steps for each UC Application node.

- a) Note down the configuration file currently active for the node (**Active File**).

You will need this information to reactivate the original configuration file at a later date.

- b) Click on the name of the respective node.

The window that contains the available configuration files opens.

- c) Click in the list entry of the `log4j_domain.xml` configuration file on

▶ to open the associated action menu.

- d) In the actions menu, select **Activate...**

The window for activating the configuration file opens.

- e) Enter your name under **Name**.

This information is logged for later research.

- f) Specify under **Reason for Activation** why you change the logging configuration of the node.

This information is logged for later research.

The window for activating the configuration file closes.

The list of system nodes displays the newly activated configuration file for the respective node under **Active File**.

- g) Click in the list entry of the respective node on ▶ to open the associated action menu.

- h) In the actions menu, select **Start new Log File**.

Logging the Domain component in a new log file thus begins.

- i) Execute these steps for each UC Application node.

After you have finished reenacting a problem, reactivate for each system node the configuration file that was active before you switched to the domain logging.

Proceed as described for the `log4j_domain.xml` configuration file.

NOTICE: You cannot activate the `default_log4j.xml` configuration file in this way. Instead, activate this configuration file by means of **Activate default configuration** in the action menu of the relevant system node.

7.1.4 Collecting Log and Dump Information automatically

This chapter provides information about the following topics:

- [The `collect.sh` Script](#)
- [logfiles-<...>.tar file](#)
- [dumpfiles-<...>.tar file](#)
- [Starting the Collection of Log and Dump Information](#)

7.1.4.1 The collect.sh Script

To collect all log and dump information of OpenScape UC Application automatically, the collect.sh script is installed along with OpenScape UC Application. You find it in the following directory:

`<Osc-Install83>/servicetools/install/bin/collect.sh`

As soon as you start collect.sh, it collects information from the log files of the various UC Application components and combines them in the following two files.

- logfiles-<host name>-<time stamp>.tar

Example: logfiles-rx300t3-2010-05-19-T164347-CEST.tar

NOTICE: You must provide this file when reporting a UC Application error through the usual error reporting mechanisms.

- dumpfiles-<host name>-<time stamp>.tar

Example: dumpfiles-rx300t3-2010-05-19-T164347-CEST.tar

Both files are saved in the /tmp/ directory.

7.1.4.2 logfiles-<...>.tar file

The logfiles-<...>.tar file contains all information that collect.sh managed to collect from the log files of the different UC Application components.

The log files file may become very large if you have collect.sh collect all log information of the various UC Application components. Therefore, you can restrict the time during which collect.sh collects log information.

7.1.4.3 dumpfiles-<...>.tar file

The dumpfiles-<...>.tar file contains heap and core dumps (memory extracts) that collect.sh managed to collect for the different UC Application components. These memory extracts can be generated in two ways:

- Automatically, in case of severe system errors – e. g. memory problems
- Manually enforced, only if especially instructed to do so by the producer's development

IMPORTANT: The generation of memory extracts may not be enforced during the productive operation of OpenScape UC Application, as after the generation, OpenScape UC Application will be in an unstable state and have to be restarted.

⁸³ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

IMPORTANT: The manually enforced generation of memory extracts may only be performed by you if you are especially instructed to do so by the producer's development.

7.1.4.4 Starting the Collection of Log and Dump Information

Start the logging of OpenScape UC Application by entering the following command. All log and dump information requested will be collected.

```
collect.sh [-hifHCDR] [-p <password>] [<start time>] [<end time>]
```

In this command the following options are available:

-h	: Displays the help information of collect.sh.
-i	: Starts collect.sh in the interactive mode which guides the user through the operation.
-f	: Starts collect.sh in the expert mode. It will be executed without any further query. This mode is only suitable for experienced users.
-h	: collect.sh collects heap dump information (memory extract).
-C	: collect.sh collects core dump information (memory extract).
-D	: Creates a new core dump (memory extract) for the computer system. <i>IMPORTANT:</i> The generation of memory extracts may not be enforced during the productive operation of OpenScape UC Application, as after the generation, OpenScape UC Application will be in an unstable state and have to be restarted. <i>IMPORTANT:</i> The manually enforced generation of memory extracts may only be performed by you if you are especially instructed to do so by the producer's development.
-R	: As last action, collect.sh restarts OpenScape UC Application on the relevant computer system. You should use this option if you have generated a memory extract, as after the generation, OpenScape UC Application will be in an unstable state and have to be restarted.
-p	: Amongst others, collect.sh performs several consistency checks some of which require a CMP administrator password. If no password is specified, collect.sh will skip the relevant consistency checks.
Start time	: collect.sh collects all log data and memory extracts generated after the time specified. <i>NOTE:</i> The <code>info date -d</code> Linux command provides a detailed description of the valid time formats.

End time	: collect.sh collects all log data and memory extracts generated before the time specified. <i>NOTE:</i> The <code>info date -d</code> Linux command provides a detailed description of the valid time formats.

You will find the files generated after the end of the script in the `/tmp/` directory.

7.1.5 Putting out Software Versions of the UC Application Components (productInventory.sh)

To put out the installed software version with its installation history on the monitor for UC Application components, the `productInventory.sh` script is installed with OpenScape UC Application.

As soon as you invoke `productInventory.sh -t` in a shell, the software versions of the UC Application components will be put out.

NOTICE: To put out the version information as a file, use the `collect.sh` script (cf. [The collect.sh Script](#) on page 615).

7.2 Logging OpenScape Voice

You find information about logging and monitoring of OpenScape Voice in the associated administrator manual.

7.3 Logging the SIP Traffic between OpenScape Voice and a Device

NOTICE: The following description assumes the presence of the network analysis software *Tethereal* on the computer system of OpenScape Voice.

The following sequence shows how to log the IP traffic on the OpenScape Voice computer system by using the *tethereal* software. You may then use the logging data to analyze the communication with a device. The trace is generated while you are logged on as **root** user on the OpenScape Voice computer system.

In the following example, the command `grep 129.103.29.202` is used to filter all lines including the traffic from and to the IP address 129.103.29.202. This address belongs to the application computer of OpenScape UC Application on which also the OpenScape Media Server is installed.

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Tue May 29 15:08:26 2007 from 129.103.148.52
pbdsa02a:~ # tethereal -n -i any |grep 129.103.29.202
```

```
tethereal: WARNING: Promiscuous mode not supported on the
"any"
device.
Capturing on Pseudo-device that captures on all interfaces
32.912888 10.76.80.102 -> 129.103.29.202 SIP/SDP Request:
  INVITE sip:998@129.103.29.202:5060;transport=UDP, with
  session description
32.951523 129.103.29.202 -> 10.76.80.102 SIP Status: 180
  Ringing
32.957619 129.103.29.202 -> 10.76.80.102 SIP/SDP Status:
  200 OK, with session description
32.958247 10.76.80.102 -> 129.103.29.202 SIP Request: ACK
  sip:129.103.29.202:5060;transport=udp
38.909059 10.76.80.102 -> 129.103.29.202 SIP Request: BYE
  sip:129.103.29.202:5060;transport=udp
38.917976 129.103.29.202 -> 10.76.80.102 SIP Status: 200 OK
```

You may also use *tethereal* as follows:

```
# tethereal -i any -n -w <binary.dumpfile>
```

Subsequently, you may analyze the data by executing the following command:

```
# ethereal <binary.dumpfile>
```

7.4 Logging OpenScape 4000

As OpenScape 4000 itself does not support the CSTA protocol, the relevant proprietary files of the system are converted to standard CSTA messages by using a OpenScape 4000 adapter. These standard CSTA messages are then logged in the symphonia. log standard logging file – analog to the OpenScape Voice messages.

When converting the proprietary files to standard CSTA messages, the adapter generates additional trace data. These trace data are written to a directory underneath the Symphonia log directory. The name of this directory has the following structure.

```
ca4000_<IP address OpenScape 4000>_<application ID>
```

Example: ca4000_10.22.100.91_7

This directory contains the following trace files you may use for error search.

- debug.log
- error.log
- trace.log
- system.log
- possibly additional backup files of the files listed

You find further information on monitoring the OpenScape 4000 systems in the *OpenScape 4000 Assistant* manuals.

7.5 Logging the Groupware Service

This chapter provides information about the following topics:

- [Log Files](#)
- [Logging Configuration](#)

7.5.1 Log Files

OpenScape UC Application saves the groupware service log files in one of the following local files.

- /var/siemens/common/log/symphony.log
- /var/siemens/common/log/symphony.log.xml

The maximum size of each of these log files is 10 MB. When this size is reached, the logging will continue in the files symphony.log.<x> or symphony.log.xml.<x>, <x> being a counter that increases by one with every new file.

Log file extract

```
2008-02-12 15:35:14,567 FINEST
[com.siemens.symphony.groupware.impl.GWServiceImpl]
GWServiceImpl - setGWBroker()
2008-02-12 15:35:14,567 DEBUG
[com.siemens.symphony.gwbackendaccess.GWBusinessLogic]
GWBusinessLogic:onSetBroker()
2008-02-12 15:35:14,569 INFO
[com.siemens.symphony.groupware.impl.GWServiceImpl]
GWServiceImpl - activate()
2008-02-12 15:35:14,569 FINEST
[com.siemens.symphony.gwbackendaccess.GWBusinessLogic]
>>>
Entering GWBusinessLogic.onActivate()
2008-02-12 15:35:14,569 DEBUG
[com.siemens.symphony.gwbackendaccess.GWBusinessLogic]
GWBusinessLogic:setBroker() -> Create GWLookup
2008-02-12 15:35:14,577 DEBUG
[com.siemens.symphony.gwlookup.impl.GWLookupSgdoImpl]
>>>GWLookupSGDOImpl(broker)
```

7.5.2 Logging Configuration

The following file allows you to configure the logging of the groupware service.

<Osc-Install⁸⁴>/common/conf/log4j.xml

In this file, the **appender-ref** Element determines if log information is saved in unstructured text files or in XML files.

- Saving log information in an unstructured text file (symphony.log)

```
<appender name="ASYNC" class="org.apache.log4j.
AsyncAppender">
```

⁸⁴ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively / enterprise/

```
<!--appender-ref ref="CONSOLE"-->  
<appender-ref ref="FILE"/>
```

- Saving log information in an XML file (symphonia.log)

```
<appender name="ASYNC" class="org.apache.log4j.  
  AsyncAppender">  
<!--appender-ref ref="CONSOLE"-->  
<appender-ref ref="FILE_XML"/>
```

In the `log4j.xml` file, you configure also which component of the groupware service is logged using which log level. These are the log levels to select.

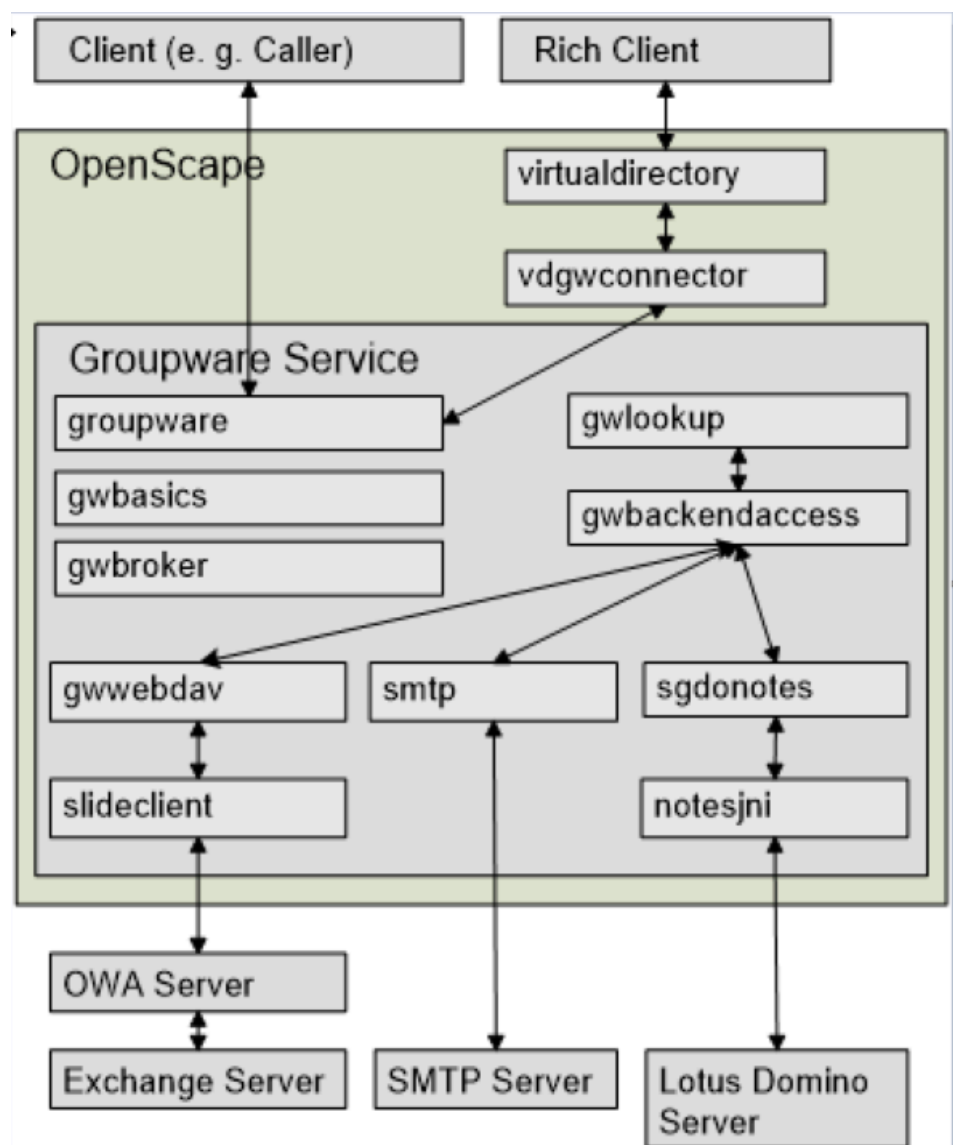
- FATAL
- ERROR
- WARN
- INFO
- DEBUG
- FINE
- FINEST

Example: Logging the gwbroker component by using the FINEST log level

```
<logger name="com.siemens.symphonia.gwbroker">  
<level value="FINEST"  
  class="com.siemens.symphonia.logging.ExtendedLevel" />  
</logger>
```

The `class="com.siemens.symphonia.logging.ExtendedLevel"` attribute is required when using the FINE or FINEST log level.

For the following components, you can configure log levels.



- gwbroker
Installing the configuration.
- groupware
Communication between the client and the groupware service.
- gwbasics
This component is used all over the groupware service. However, it barely generates log messages.
- gwbackendaccess
Communication between the groupware service and the IBM Lotus Domino Server or Microsoft Exchange Server. This component communicates with the components sgdonotes, gwlookup and smtp.

- Communication between the groupware service and the Microsoft Exchange Server.
 - slideclient
Command execution layer between gwwebdav and the Microsoft Exchange Server.
 - smtp
Sending anonymous e-mails.
- Communication between the groupware service and the IBM Lotus Domino Server.
 - sgdonotes
SGDO stands for Simple Group Data Objects. This component contains the logic for the communication between the groupware service and the IBM Lotus Domino Server. It communicates with gwbackendaccess and notesjni.
 - notesjni
command execution from Java to C++ between the component sgdonotes and the IBM Lotus Domino Server
- Contacts
 - virtualdirectory
The OpenScape UC Application contact data base.
 - vdgwconnector
This component provides OpenScape UC Application the access to the groupware contacts.
 - gwlookup
gwbackendaccess can invoke gwlookup, the cache and index for contacts to obtain contacts sorted by phone numbers or name dialing phone numbers.

NOTICE: If you report an error in the groupware service, you should always send a log file you generated by using the FINEST log level.

IMPORTANT: The logging of the groupware service may require an important percentage of the processing power of the UC Application system. This may deteriorate the system performance from the point of view of the user. Therefore, activate the logging only for the time required to search for an error. Furthermore, only activate the log levels really required for the error search.

7.6 Logging the Web Server Component

This chapter provides information about the following topics:

- [Concept of the Web Server Component Logging](#)

- [Determining Additional Data for Logging](#)
- [Reproducing a Problem Using the Web Server Component](#)
- [Logging the OpenScape Desktop Integration Tool](#)

7.6.1 Concept of the Web Server Component Logging

The web server component of OpenScape UC Application uses the logging mechanism and the logging files which are also used by the ComAssistant. The logging of the web server component is thus independent of the Symphonia logging.

The logging levels from **0** to **5** are defined as follows.

- 0 - FATAL
- 1 - ERROR
- 2 - WARNING
- 3 - MESSAGE
- 4 - TRACE
- 5 - DEBUG_TRACE

For the logging functions, the installation directory of the web server component contains the following structures.

- `<Osc-Install85>/HiPathCA/config/common/global.cfg`

In this file, the first part of the following section determines the settings for Integrated Deployment, the second part determines the settings for all other deployment scenarios.

Log size depending on 8k scenario

The settings for Integrated Deployment follow from here:

```
<?x if(<?x $IS_HP8K ?> == "1") ?>
<?x setvar (LOG_INIT_LEVEL4J = "3" ) ?>
<?x setvar (LOG_INIT_ = "3" ) ?>
<?x setvar (LOG_INIT_ = "3" ) ?>
<?x else ?>
```

The settings for all other deployment scenarios follow from here:

```
<?x setvar (LOG_INIT_LEVEL4J = "5" ) ?>
<?x setvar (LOG_INIT_ = "3" ) ?>
<?x setvar (LOG_INIT_ = "5" ) ?>
<?x endif ?>
```

- The **LOG_INIT_LEVEL** variable, which depends on the scenario, specifies the general log level. The values allowed are between **0** and **5**, **5** providing the most detailed output.
- The **LOG_INIT_LEVEL4J** variable, which depends on the scenario, specifies the log level for the internally created appender. The values allowed are between **1** and **5**, **5** providing the most detailed output.

⁸⁵ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

- The **LOG_INIT_MAXDAYS** variable, which depends on the scenario, specifies for how many days the logging files for the web server component will be saved. The values allowed are between **1** and **10**.

IMPORTANT: If you configure for this setting a value greater than **10**, the logging files may need so much space on the hard disk that OpenScape UC Application will not work correctly any more.

- `<Osc-Install>/HiPathCA/config/<host name>/`
This directory contains processes or services to be started on the `<host name>` computer.
- `<Osc-Install>/HiPathCA/config/<host name>/<procname>.proc`
This file contains command information interpreted by the process controller to execute a new process.
- `<Osc-Install>/HiPathCA/config/<host name>/<service name>.svc`
This file contains information on the service instantiation and the start parameters interpreted by the service controller.
- `<Osc-Install>/HiPathCA/config/services/default/<serviceType>/`
This directory contains configuration parameters for a service of the `<serviceType>` type.
- `<Osc-Install>/HiPathCA/config/services/default/ServiceController/default/resources/log4j.xml`
The information in this file provides the fine grain control of the log4j output.
- `/var/siemens/common/log/webclient/<date>/ or /log/webclient/<date>/`
• `/var/siemens/common/log/webclient/openscapeuc/<date>/ or /log/webclient/openscapeuc/<date>/`
These directories contain the logging files for OpenScape Web Client collected by different loggers on day `<date>`.

7.6.2 Determining Additional Data for Logging

How to determine which additional data should be included when logging the web server component:

- 1) End the **WebClient** service on the OpenScape UC Application application computer by executing the following command:
`/etc/init.d/symphoniad stop WebClient`

NOTICE: If you use a deployment scenario with several UC Application computer systems, deploy the `stop WebClient_BE` command on the application computer.

- 2) check if `net.openscape.webclient` logger exists.

if it does not exist, then add to `<Lync-Install86>/HiPathCA/config/common/log4j-webtier.xml` the the following lines:

```
<root>
<priority value="UNEXPECTED"
  class="com.cycos.media.logging.log4j.ExtendedLevel"/>
<appender-ref ref="DAILYROLL"/>
</root>
```

- 3) To activate the XML trace, proceed as follows.

- a) Open the following file.

```
<Lync-Install86>/HiPathCA/config/services/default/
PSMService/PSM.cfg
```

- b) In the file, remove the # comment marker.

- c) Configure the following parameter

```
xml.traceSubDir = xml
:
```

- 4) Activate global logging as follows.

- a) Open the following file.

```
<Lync-Install86>/HiPathCA/config/common/global.cfg
```

- b) Depending on the deployment scenario used, configure the following variable:

For Integrated Deployment:

```
# Log size depending on 8k scenario
<?x if(<?x $IS_HP8K ?> == "1") ?>
<?x setvar (LOG_INIT_LEVEL4J = "3" ) ?>
<?x setvar (LOG_INIT_LEVEL = "5" ) ?> ...
```

For all other deployment scenarios:

```
# Log size depending on 8k scenario
<?x if(<?x $IS_HP8K ?> == "1") ?>
...
<?x else ?> <?x setvar (LOG_INIT_LEVEL4J = "5" ) ?>
<?x setvar (LOG_INIT_LEVEL = "5" ) ?>
...
```

- 5) Start the **WebClient** service on the OpenScape UC Application application computer by executing the following command:

```
/etc/init.d/symphoniad start WebClient
```

NOTICE: If you use a deployment scenario with several UC Application computer systems, deploy the start `WebClient_BE` command on the application computer.

⁸⁶ `<Lync-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `enterprise/`

6) If you use OpenScape Web Client, activate the detailed log as follows:

a) Open the following file on the front-end computer system:

Up to and inclusive OpenScape UC Application V7R2 **FR0**:

```
<Osc-Install>/HiPathCA/config/services/default/  
ServiceController/default/resources/log4j.xml
```

As of OpenScape UC Application V7R2 **FR1**:

```
<Osc-Install>/HiPathCA/config/common/log4j-webtier.xml
```

b) Set the value for the **level value** parameter to **ALL** for the **net.openscape.webclient** logger.

Example:

```
<logger name="net.openscape.webclient">  
<level value="ALL"/>  
<appender-ref ref="R"/>  
</logger>
```

c) Execute these steps on every available front-end computer system.

7.6.3 Reproducing a Problem Using the Web Server Component

How to reproduce a problem using the web server component:

1) End the **WebClient** service on the OpenScape UC Application application computer by executing the following command:

```
/etc/init.d/symphoniad stop WebClient
```

NOTICE: If you use a deployment scenario with several UC Application computer systems, deploy the `stop WebClient_BE` command on the application computer.

2) Delete the following directory completely.

For Integrated Deployment:

```
/var/siemens/common/log/webclient
```

For all other deployment scenarios:

```
/log/webclient
```

3) Start the **WebClient** service on the OpenScape UC Application application computer by executing the following command:

```
/etc/init.d/symphoniad start WebClient
```

NOTICE: If you use a deployment scenario with several UC Application computer systems, deploy the `start WebClient_BE` command on the application computer.

4) Reproduce the problem to log the diagnostics data.

- 5) Compress the following directories in a ZIP file named sysdiag.zip.
 - `<Wc-Install87>/config`
 - `/var/siemens/common/log/webclient` or
`/log/webclient`
- 6) Create an MR (CQ) containing a clear error description and all version information and add the sysdiag.zip file as attachment to the MR (CQ).
- 7) In order to save system resources, revert the changes you made to the `cfg` and `xml` files in [Determining Additional Data for Logging](#) on page 624 and execute the following command:
`/etc/init.d/symphoniad restart WebClient`

NOTICE: If you use a deployment scenario with several UC Application computer systems, deploy the `restart WebClient_BE` command on the application computer.

NOTICE:

A mechanism, introduced in V9R4 FR38 and also included in all V11 lines, allows to reload the log4j configuration for the WebClient FE logs (openscapeuc logs) without needing to restart the complete WebClient service.

Please note that this does not involve the WebClient BE logs (`/opt/siemens/HiPathCA/config/common/global.cfg`) which will still require a restart of the BE server.

Please also keep in mind that the log file is not rolled over after a log4j reload. With this mechanism the administrator will be able to reload the log4j settings after having manually edited the `log4j-webtier.xml` file (located in `/opt/siemens/HiPathCA/config/common/log4j-webtier.xml` on each FE node or in the offboard node in case of a Small deployment).

After that in order to reload the updated log4j configurations the following script should be executed for each FE node (or in the offboard node in case of a Small deployment): `/opt/siemens/HiPathCA/bin/reloadWebLog4j.sh`

7.6.4 Logging the OpenScape Desktop Integration Tool

This chapter provides information about the following topics:

- [Concept of the OpenScape Desktop Integration Tool Logging](#)
- [Activating the Logging for OpenScape Desktop Integration Tool across the System](#)
- [Activating the Logging for OpenScape Desktop Integration Tool specific to Clients](#)

⁸⁷ `<Wc-Install>` is the web server setup directory: `/opt/siemens/HiPathCA` or `/enterprise/HiPathCA`

7.6.4.1 Concept of the OpenScape Desktop Integration Tool Logging

The OpenScape Desktop Integration tool uses its own logging mechanism and logging files. The logging of the OpenScape Desktop Integration tool is thus independent of the Symphonia logging.

The OpenScape Desktop Integration tool uses log levels from **0** to **5**. They are defined as follows.

- 0 - Logging deactivated
- 1 - FATAL
- 2 - ERROR
- 3 - WARNING
- 4 - MESSAGE
- 5 - DEBUG_TRACE (for developer analysis)

The logging level used can be found on the user PC in the following file under the parameter **DEPLOYMENT_LOGLEVEL**, but it cannot be changed.

%appdata%\Siemens\OSCWebDI.deployment

Logging for the OpenScape Desktop Integration Tool and the corresponding log level can be configured in the following file across the system and for all users.

<Osc-Install⁸⁸>/HiPathCA/config/deployment.props

Furthermore, logging can also be started specific to a client in the desired client. In this case, log level **5** applies always.

Furthermore, logging the OpenScape Desktop Integration Tool writes the collected log data in the following log files. The maximum size of each of them is 1 MB.

- OSCWebDI.log

This file is used to log all current information.

As soon as this file reaches the size of 1 MB, it is renamed to OSCWebDI.log.last0.log, the file OSCWebDI.log.last0.log to OSCWebDI.log.last1.log etc.

- Files with names of the following format: OSCWebDI.log.last<x>.log

These are archive files that store previous information.

The maximum number of these files that may exist is determined by the logging level used. The following applies: The maximum number of existing archive files is equal to the logging level number.

Example:

The log level used is **4**. In this case, the number of archive files is limited to four. OSCWebDI.log.last0.log to OSCWebDI.log.last3.log.

All logging files are stored in the following directory on the user PC.

%appdata%\Siemens

⁸⁸ <Osc-Install> is the setup directory of OpenScape UC Application: /opt/siemens/ respectively /enterprise/

7.6.4.2 Activating the Logging for OpenScape Desktop Integration Tool across the System

How to activate the logging for OpenScape Desktop Integration Tool or to change the log level used for all users:

- 1) Open the following configuration file with a text editor:

`deployment.props`

You find this file in the following folder of the application computer:

`<Osc-Install89>/HiPathCA/config/`

- 2) Under **DI_LOGLEVEL**, enter the value for the desired logging level.
- 3) Save the changes in the configuration file.
- 4) Open a shell on the application computer and execute the following command to restart the web server component.

`/etc/init.d/symphoniad restart WebClient`

The web server component stops and immediately reboots again.

The setting is transmitted automatically to all user PCs involved and will be activated on the next startup of the corresponding OpenScape Desktop Integration tool.

NOTICE: User PCs must have write access to the OpenScape Desktop Integration tool deployment folder in order to be able to start and update the Client. You can find details on how to install the OpenScape Desktop Integration tool in the OpenScape UC Application, Installation and Upgrade manual.

7.6.4.3 Activating the Logging for OpenScape Desktop Integration Tool specific to Clients

How to activate the logging for OpenScape Desktop Integration Tool specific to clients:

- 1) Stop the relevant OpenScape Desktop Integration Tool on the user PC.
- 2) Open the following configuration file with a text editor:

`OSCWebDI.cfg`

You find this file in the following folder of the user computer:

`%appdata%\Siemens`

- 3) Attach the following line to the end of the available text:

`DEBUG=1`

- 4) Save the changes in the configuration file.
- 5) Start OpenScape Desktop Integration Tool.

⁸⁹ `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

System Monitoring

Logging Nuance Vocalizer (TTS)

6) In the notification area of the Windows desktop, click with the right mouse button on the OpenScape Desktop Integration Tool icon to open the context menu.

7) Select the **DEBUG** item in the context menu.

The dialog with the debug settings opens.

8) Select **LOG:Debug** and close the dialog.

Logging starts with log level **5** for the relevant OpenScape Desktop Integration Tool.

The next time OpenScape Desktop Integration Tool launches, this logging setting will be reset to the default value that results from the central logging configuration. See [Activating the Logging for OpenScape Desktop Integration Tool across the System](#) on page 629 on this.

7.7 Logging Nuance Vocalizer (TTS)

You find information about how to log the TTS system of producer Nuance in the associated product information of the producer.

7.8 Compression of Log-files for WebClient

Normally the log-files during one day are being compressed.

However, if the size of the folder exceeds 600 MBs in one day then the folder is not compressed.

Folders are under

`/var/siemens/common/log/webclient` or `/log/webclient`.

8 Statistics Data

This chapter provides information about the following topics:

- [Raw Statistics Output of the Conference Portal](#)
- [Raw Statistics Output of the OpenScape Media Server](#)

8.1 Raw Statistics Output of the Conference Portal

This chapter provides information about the following topics:

- [Statistics Concept of the Conference Portal](#)
- [Structure of the Conference Portal Statistics Data](#)
- [Activating the Raw Statistics Output for the Conference Portal](#)
- [Configuring the Output Settings for the Conference Portal Raw Statistics](#)

8.1.1 Statistics Concept of the Conference Portal

The conference portal uses the OpenScape Media Server statistics framework to collect event-related statistics data for the current operation of the conference portal. The statistics data collected comprise information on internally used conference portal entities and their interaction. The information collected is provided by the statistics framework in the form of raw statistics.

The raw statistics can be used especially for the following purposes:

- To provide real-time monitoring of the most important conference entities.
- To create individual statistics reports in order to determine the communication behavior and the load of the conference portal.
- To create entity and sequence diagrams that help optimizing error analysis and bug fixing.

The conference portal puts out the raw statistics data collected using the Round-Robin procedure. By default, it uses a file system consisting of ten files each of which may reach a default maximum size of 10 MB.

The files of the file system are stored in the following directory of the OpenScape Media Server.

<MS-Install⁹⁰>/logs/traces

By default, the statistics files have the following names:

conferencing-statistic.log.<sequential number>

The output of the raw statistics data collected can be configured by using the OpenScape service **Conferencing Statistics**.

The raw statistics data put out can be processed as required by using an external statistics application.

⁹⁰ <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ respectively /enterprise/

8.1.2 Structure of the Conference Portal Statistics Data

The statistics messages about the current operation of the conference portal are event-related. The following conference portal events are relevant.

Conference events

- ConferenceStartedEvent

This event occurs when a conference is started. The statistics messages following this event are described in [Statistics Messages for the Event ConferenceStartedEvent](#) on page 635.

- ConferenceStoppedEvent

This event occurs when a conference is ended. The statistics messages following this event are described in [Statistics Messages for the Event ConferenceStoppedEvent](#) on page 638.

- ConferenceProlongedEvent

This event occurs when the duration of a conference is prolonged. The statistics messages following this event are described in [Statistics Messages for the Event ConferenceProlongedEvent](#) on page 638.

- VoiceConferenceAddedEvent

This event occurs when an audio conference is added to an existing conference. The statistics messages following this event are described in [Statistics Messages for the Event VoiceConferenceAddedEvent](#) on page 639.

- WebConferenceAddedEvent

This event occurs when a web conference is added to an existing conference. The statistics messages following this event are described in [Statistics Messages for the Event VideoConferenceAddedEvent](#) on page 639.

- VideoConferenceAddedEvent

This event occurs when a video conference is added to an existing conference. The statistics messages following this event are described in [Statistics Messages for the Event WebConferenceAddedEvent](#) on page 640.

User events

- UserState_Joined

This event occurs when a user joins a voice, web or video conference. The statistics messages following this event are described in [Statistics Messages for the Event UserState_Joined](#) on page 640.

- UserState_Left

This event occurs when a user leaves a voice, web or video conference. The statistics messages following this event are described in [Statistics Messages for the Event UserState_Left](#) on page 641.

- UserState_Rejected

This event occurs when a user is called to join a voice, web or video conference, but rejects the call. The statistics messages following this event are described in [Statistics Messages for the Event UserState_Rejected](#) on page 641.

- UserConnectingFailedEvent

This event occurs when a user cannot join a conference because his/her connection to the conference portal has been refused or has failed. The statistics messages following this event are described in [Statistics Messages for the Event userconnectingfailedEvent](#) on page 642.

- UserAddedEvent

This event occurs when a user is invited to a conference through the OpenScape Web Client.

NOTICE: With this event, the user has not joined the conference yet. This will only occur with the UserState_Joined event.

The statistics messages following this event are described in [Statistics Messages for the Event UserAddedEvent](#) on page 642.

Statistics messages and their format

Each of the events listed creates at least one statistics message in the following general form.

<entry length>,<time>,<entity type>,<entity ID>,<message type>,<possibly data depending on the message>

Example:

```
70,03.12.2010
14:35:58.323,conf.conference,conf.conference.1,ATTRIBUTE,
DURATION,60,,
```

Possible entity types

Currently, conferences and users are used as entities. The following entity types are assigned to them.

Entity	Entity type
Conference	conf.conference
User	conf.user
Call	conf.call

Possible message types

Each statistics message belongs to one of the following message types:

- ATTRIBUT

A statistics message of this type puts out attribute values for the entity defined by *<entity ID>*. Each statistics entry of this type documents the

information of an attribute. In doing so, a data pair consisting of attribute name and attribute value is put out.

Example:

Attribute output for the conference entity with the entity ID

conf.conference.1. The attribute name is **DURATION**, the attribute value is **60**

81, <time>, conf.conference, conf.conference.1, ATTRIBUTE, DURATION, 60, ,

- CREATE

A statistics message of this type documents the creation of the entity the type of which is defined by <entity type> and its ID by <entity ID>.

Example:

Creation of the user entity with the entity ID **conf.user.1**

57, <time>, conf.user, conf.user.1, CREATE, , , ,

- DESTROY

A statistics message of this type documents the creation of the entity the type of which is defined by <entity type> and its ID by <entity ID>.

Example:

Deletion of the conference entity with the entity ID **conf.conference.1**

69, <time>, conf.conference, conf.conference.1, DESTROY, , , ,

- INVOKED

A statistics message of this type documents the occurrence of a specified event for the entity defined by <entity ID>.

Example:

Conference entity with the entity ID **conf.conference.1** *was started*

64, <time>, conf.conference, conf.conference.1, INVOKED, START_VOICE, , ,

- REFERENCE

A statistics message of this type can have two purposes:

- To document to which conference a user belongs. In this case, the <message type> is followed by the text **CONFERENCE**.

Example:

Attribution of the user entity with the entity ID **conf.user.1** *to the conference entity with the entity ID* **conf.conference.1**

102, <time>, conf.user, conf.user.1, REFERENCE, CONFERENCE, conf.conference.1,

- To document the creator of a conference. In this case, the <message type> is followed by the text **CREATOR**.

Example:

Attribution of the user entity with the entity ID **conf.user.1** *to the conference entity with the entity ID* **conf.conference.1**.

88, <time>, conf.conference, conf.conference.1, REFERENCE, CREATOR, conf.user.1,

8.1.2.1 Statistics Messages for the Event ConferenceStartedEvent

The event ConferenceStartedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type CREATE](#)
- [Message type ATTRIBUTE](#)
- [Message type REFERENCE](#)

Message type INVOKED

Message indicating the general occurrence of the event ConferenceStartedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, START_VOICE, , ,
```

Message type CREATE

Message about the creation of the conference entity and the corresponding user entities.

Example:

```
57, <time>, conf.conference, conf.conference.1, CREATE, , , ,
```

...

```
57, <time>, conf.user, conf.user.1, CREATE, , , ,
```

Message type ATTRIBUTE

Message for the following attributes of the started conference entity and the corresponding user entities.

Entity	Attribute name	Contents	Possible values
Conference	CONFERENCE_ID	Indicates the ID of the relevant conference.	<conference ID>
	TITLE	Indicates the title of the relevant conference.	<conference title>
	IS_MODERATED	Indicates if the conference is a moderated one.	[true false]
	IS_ADHOC	Indicates if the conference is an Ad-hoc conference.	[true false]
	IS_SERIES	Indicates if the conference is a recurring one.	[true false]
	SCHEDULED_TIME	Indicates when the conference starts.	<time in hh:mm format>
	DURATION	Indicates how long the conference lasts.	<duration in minutes>
	HAS_VOICE	Indicates if the conference comprises audio streaming.	[true false]

Entity	Attribute name	Contents	Possible values
	AUDIO_PIN	Indicates the PIN for logging on to the audio streaming.	<PIN>
	HAS_WEB	Indicates if the conference comprises a web conference.	[true false]
	HAS_VIDEO	Indicates if the conference comprises video streaming.	[true false]
	STARTED_BY	Indicates the interface through which the conference is started.	[CLIENT SCHEDULER TUI]

Example:

```

75,<time>,conf.conference,0,ATTRIBUTE,CONFERENCE_ID,conf.13,,
79,<time>,conf.conference,0,ATTRIBUTE,TITLE,testVoiceConference,,
72,<time>,conf.conference,0,ATTRIBUTE,IS_MODERATED,false,,
68,<time>,conf.conference,0,ATTRIBUTE,IS_ADHOC,false,,
69,<time>,conf.conference,0,ATTRIBUTE,IS_SERIES,false,,
69,<time>,conf.conference,0,ATTRIBUTE,SCHEDULED_TIME,,,
65,<time>,conf.conference,0,ATTRIBUTE,DURATION,30,,
68,<time>,conf.conference,0,ATTRIBUTE,HAS_VOICE,true,,
70,<time>,conf.conference,0,ATTRIBUTE,AUDIO_PIN,267886,,
67,<time>,conf.conference,0,ATTRIBUTE,HAS_WEB,false,,
69,<time>,conf.conference,0,ATTRIBUTE,HAS_VIDEO,false,,
71,<time>,conf.conference,0,ATTRIBUTE,STARTED_BY,Client,,

```

Entity	Attribute name	Contents	Possible values
User	DISPLAY_NAME	Indicates the display name of the user.	<display name>
	EMAIL_ADDRESS	Indicates the e-mail address of the user.	<E-mail address>
	ROLE	Indicates the role of the user for the conference.	[MODERATOR PARTICIPANT]
	LANGUAGE	Indicates the language of the user.	<token of a system language>
	TYPE	Indicates if the user is an OpenScape user or not.	[DOMAIN EXTERNAL]
	IS_DIAL_IN	Indicates if the user dials into the conference by himself/herself or is called by the OpenScape system. Only used if audio streaming is used.	[true false]
	ONS_NUMBER	Indicates the ONS number of the user. Only used if audio streaming is used.	<phone number in normalized format>

Example:

```

84,<time>,conf.user,conf.user.1,ATTRIBUTE,DISPLAY_NAME,User1,,

```



```

73,<time>,conf.user,conf.user.1,ATTRIBUTE,EMAIL_ADDRESS,,,
75,<time>,conf.user,conf.user.1,ATTRIBUTE,ROLE,PARTICIPANT,,
68,<time>,conf.user,conf.user.1,ATTRIBUTE,LANGUAGE,en_us,,
72,<time>,conf.user,conf.user.1,ATTRIBUTE,TYPE,Domain,,
73,<time>,conf.user,conf.user.1,ATTRIBUTE,ONS_NUMBER,+4924041231513,,
75,<time>,conf.user,conf.user.1,REFERENCE,CONFERENCE,conf.conference,0,

```

Entity	Attribute name	Contents	Possible values
Call	IP	The IP address of the device	<ip>
	PHONE_NUMBER	Phone number of the device	<Phone Number>
	IS_DIAL_IN	True if device has dial in the conferencing bridge	[true false]
	CALL_IN_TERMINAL	The terminal it was used in case of a dial-in call	<Terminal>
	CALL_OUT_TERMINAL	The terminal it was used in case of a dial-out call	<Terminal>
	PREVIOUS_NODE_IP	If the call was transferred from another MS node the IP address of the previous node	<ip>
	PREVIOUS_SESSION_ID	If the call was transferred from another MS node the session-id it was assigned from the previous node	<Session ID>
	TRANSFERRING	True if call is being transferring	[true false]
	TRANSFERRED	True if call was transferred	[true false]
	STARTING_TIME	Timestamp when the call was initiated	<Time Stamp>
	ENDING_TIME	Timestamp when the call was terminated	<Time Stamp>

Example:

```

<time>,conf.call,conf.call.99,CREATE,,,,
<time>,conf.call,conf.call.99,ATTRIBUTE,IP,172.25.8.68,,
<time>,conf.call,conf.call.99,ATTRIBUTE,VOICE_SESSION_ID,session:sid.158,,
<time>,conf.call,conf.call.99,ATTRIBUTE,PHONE_NUMBER,+4989700728207,,
<time>,conf.call,conf.call.99,ATTRIBUTE,IS_DIAL_IN,true,,
<time>,conf.call,conf.call.99,ATTRIBUTE,CALL_IN_TERMINAL,+4989700731505,,
<time>,conf.call,conf.call.99,ATTRIBUTE,CALL_OUT_TERMINAL,+302108189708,,
<time>,conf.call,conf.call.99,ATTRIBUTE,STARTING_TIME,1503387068695,,
<time>,conf.call,conf.call.99,ATTRIBUTE,TRANSFERRING,false,,
<time>,conf.call,conf.call.99,ATTRIBUTE,TRANSFERRED,false,,
<time>,conf.call,conf.call.99,INVOKED,ESTABLISH,,,
<time>,conf.call,conf.call.99,ATTRIBUTE,ENDING_TIME,1503387074870,,
<time>,conf.call,conf.call.99,INVOKED,TERMINATE,,,
<time>,conf.call,conf.call.99,DESTROY,,,,

```

Message type REFERENCE

Message about the creator of a conference or the conference a user belongs to.

Example:

```
88, <time>, conf.conference, 0, REFERENCE, CREATOR, conf.user, conf.user.1,
102, <time>, conf.user, conf.user.1, REFERENCE, CONFERENCE, conf.conference, 0
```

8.1.2.2 Statistics Messages for the Event ConferenceStoppedEvent

The event ConferenceStoppedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type DESTROY](#)

Message type INVOKED

Message indicating the general occurrence of the event ConferenceStoppedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, STOP_VOICE, , ,
```

Message type DESTROY

Message about the Deletion of the conference entity and the corresponding user entities.

Example:

```
57, <time>, conf.conference, conf.conference.1, DESTROY, , , ,
```

...

```
57, <time>, conf.user, conf.user.1, DESTROY, , , ,
```

8.1.2.3 Statistics Messages for the Event ConferenceProlongedEvent

The event ConferenceProlongedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type ATTRIBUTE](#)

Message type INVOKED

Message indicating the general occurrence of the event ConferenceProlongedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, PROLONGED, , ,
```

Message type ATTRIBUTE

Message for the DURATION attribute determining the prolongation of the conference duration in minutes.

Example:

```
82, <time>, conf.conference, conf.conference.1, ATTRIBUTE, DURATION, 60,
```

8.1.2.4 Statistics Messages for the Event VoiceConferenceAddedEvent

The event VoiceConferenceAddedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type ATTRIBUTE](#)

Message type INVOKED

Message indicating the general occurrence of the event VoiceConferenceAddedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, VOICE_CONFERENCE,
```

Message type ATTRIBUTE

Message for the modified attributes HAS_VOICE and AUDIO_PIN of the corresponding conference.

Example:

```
68, <time>, conf.conference, 0, ATTRIBUTE, HAS_VOICE, true, ,
70, <time>, onf.conference, 0, ATTRIBUTE, AUDIO_PIN, 267886, ,
```

8.1.2.5 Statistics Messages for the Event VideoConferenceAddedEvent

The event VideoConferenceAddedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type ATTRIBUTE](#)

Message type INVOKED

Message indicating the general occurrence of the event VideoConferenceAddedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, VIDEO_CONFERENCE,
```

Message type ATTRIBUTE

Message for the changed attribute HAS_VIDEO of the corresponding conference.

Example:

```
68, <time>, conf.conference, 0, ATTRIBUTE, HAS_VIDEO, true, ,
```

8.1.2.6 Statistics Messages for the Event WebConferenceAddedEvent

The event WebConferenceAddedEvent creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type ATTRIBUTE](#)

Message type INVOKED

Message indicating the general occurrence of the event WebConferenceAddedEvent.

Example:

```
64, <time>, conf.conference, conf.conference.1, INVOKED, WEB_CONFERENCE_ADD
```

Message type ATTRIBUTE

Message for the changed attribute HAS_WEB of the corresponding conference.

Example:

```
68, <time>, conf.conference, 0, ATTRIBUTE, HAS_WEB, true,,
```

8.1.2.7 Statistics Messages for the Event UserState_Joined

The event UserState_Joined creates statistics messages of the following message types.

- [Message type INVOKED](#)
- [Message type ATTRIBUTE](#)

Message type INVOKED

Message about the general occurrence of the event UserState_Joined when a user joins a voice conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, JOINED_VOICE, conf.conference, conf.conferen
```

Message about the general occurrence of the event UserState_Joined when a user joins a video conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, JOINED_VIDEO, conf.conference, conf.conferen
```

Message about the general occurrence of the event UserState_Joined when a user joins a web conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, JOINED_WEB, conf.conference, conf.conferen
```

Message type ATTRIBUTE

Message for the changed attributes IN_BOUND and DIAL_IN_NUMBER of the relevant user when he/she joins a voice conference.

Example:

```
72, <time>, conf.user, conf.user.1, ATTRIBUTE, IN_BOUND, true,,
```

```
88, <time>, conf.user, conf.user.1, ATTRIBUTE, DIAL_OUT_NUMBER,
+4924041231841, ,
```

8.1.2.8 Statistics Messages for the Event UserState_Left

The event UserState_Left creates statistics messages of the following message types.

- [Message type INVOKED](#)

Message type INVOKED

Message about the general occurrence of the event UserState_Left when a user leaves a voice conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, LEFT_VOICE, conf.conference, conf.conf
```

Message about the general occurrence of the event UserState_Left when a user leaves a video conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, LEFT_VIDEO, conf.conference, conf.conf
```

Message about the general occurrence of the event UserState_Left when a user leaves a web conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, LEFT_WEB, conf.conference, conf.conf
```

8.1.2.9 Statistics Messages for the Event UserState_Rejected

The event UserState_Rejected creates statistics messages of the following message types.

- [Message type INVOKED](#)

Message type INVOKED

Message about the general occurrence of the event UserState_Rejected when a user rejects a voice conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, REJECTED_VOICE, conf.conference, conf.conf
```

Message about the general occurrence of the event UserState_Rejected when a user rejects a video conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, REJECTED_VIDEO, conf.conference, conf.conf
```

Message about the general occurrence of the event UserState_Rejected when a user rejects a web conference.

Example:

```
75, <time>, conf.user, 1, INVOKED, REJECTED_WEB, conf.conference, conf.conf
```

8.1.2.10 Statistics Messages for the Event `userconnectingfailedEvent`

The event `UserConnectingFailedEvent` creates statistics messages of the following message type:

- [Message type INVOKED](#)

Message type INVOKED

Message about the general occurrence of the event `UserConnectingFailedEvent` when a user cannot join a voice conference because his/her connecting to the conference portal was rejected or failed.

Example:

```
109, <time>, conf.user, 4, INVOKED, USER_CONNECTING_FAILED_VOICE, <rejection reason>, conf.conference, conf.conference.1
```

Message about the general occurrence of the event `UserConnectingFailedEvent` when a user cannot join a video conference because his/her connecting to the conference portal was rejected or failed.

Example:

```
109, <time>, conf.user, 4, INVOKED, USER_CONNECTING_FAILED_VIDEO, <rejection reason>, conf.conference, conf.conference.1
```

Message about the general occurrence of the event `UserConnectingFailedEvent` when a user cannot join a web conference because his/her connecting to the conference portal was rejected or failed.

Example:

```
109, <time>, conf.user, 4, INVOKED, USER_CONNECTING_FAILED_WEB, <rejection reason>, conf.conference, conf.conference.1
```

In these INVOKED messages, one of the following specifications can be put out as `<rejection reason>`.

- General Call Error
- Empty Callout address
- Domain user has no phone number
- Address incomplete
- Call not acceptable
- Ring timeout
- Busy
- Not Found
- User dialog timeout

8.1.2.11 Statistics Messages for the Event `UserAddedEvent`

The event `UserAddedEvent` creates statistics messages of the following message types.

- [Message type INVOKED](#)

Message type INVOKED

Message about the general occurrence of the event `UserAddedEvent` when a user is invited to a conference through the OpenScape Web Client.

NOTICE: With this event, the user has not joined the conference yet. This will only occur with the `UserState_Joined` event.

Example:

`73, <time>, conf.user, 3, INVOKED, USER_ADDED, conf.conference, conf.conf`

8.1.3 Activating the Raw Statistics Output for the Conference Portal

How to activate the statistics output for the conference portal:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click on the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Conferencing Statistics** component and click on the associated component name.

The dialog with the settings of the conference statistics component opens.

- 6) Specify the **true** value under **EnableStatistics**.
- 7) Select **Save** to copy the new settings.

You have thus activated the statistics output for the conference portal.

8.1.4 Configuring the Output Settings for the Conference Portal Raw Statistics

How to configure the output settings for the conference portal raw statistics:

- 1) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 2) In the navigation tree, click on **Nodes & Applications > Nodes**.

A list of all system nodes and external links available in the entire system is displayed in the workspace.

- 3) Click on the name of the system node on which OpenScape UC Application is installed.

A dialog with the dashboard of the selected node opens.

- 4) Click on **Show** next to **Actions – Show services status**.

A dialog opens with a list of all components available for the selected system node.

The **State** column displays whether the component is started  or

stopped .

- 5) Search the list for the **Conferencing Statistics** component and click on the associated component name.

The dialog with the settings of the conference statistics component opens.

- 6) Under **FileName**, specify the file name under which the raw statistics files should be saved.

NOTICE: The raw statistics files created will always be stored in the following OpenScape Media Server directory:
<MS-Install⁹¹>/logs/traces

- 7) Under **FileSize**, specify the maximum size of the raw statistics files Use the following units: **MB**, **GB** or **TB**.

Example: 100MB

NOTICE: If you specify a number without unit, the corresponding value will be interpreted as a value in KB.

- 8) Under **NumberOfFiles**, specify the number of raw statistics files to be used for the Round-Robin output.
- 9) If you would like to activate the statistics output for the conference portal at the same time, enter under **EnableStatistics** the **true** value.
- 10) Select **Save** to copy the new settings.

IMPORTANT: By the following step, all OpenScape UC Application services are stopped without any further prompt and immediately restarted. This interrupts the OpenScape UC Application services for some minutes.

- 11) Execute the following command to have the changed settings become effective:

```
/etc/init.d/symphoniad restart
```

You have thus configured the output settings for the conference portal raw statistics.

8.2 Raw Statistics Output of the OpenScape Media Server

You find information about OpenScape Media Server statistics data in the *OpenScape Media Server, Administrator Documentation* manual.

⁹¹ <MS-Install > is the setup directory of the OpenScape Media Server: /opt/siemens/ respectively / enterprise/

9 Upgrading external Systems

You can operate various external systems at OpenScape UC Application – for example the communications system OpenScape Voice.

This chapter tells you which configuration steps you must execute for upgrading such an external system.

You must execute configuration steps for the following upgrade scenarios:

- [Upgrading HiPath 4000 V6 to OpenScape 4000 V7](#) on page 645

9.1 Upgrading HiPath 4000 V6 to OpenScape 4000 V7

Execute the following configuration steps if you operate at OpenScape UC Application a Hipath 4000 V6 system you have upgraded to OpenScape 4000 V7:

- 1) Start OpenScape 4000 Assistant.
- 2) Select **Base Administration > Application Control** in the launch pad.
- 3) Activate the check box of the **Import / Export API (XIE)** application and save the modification.
- 4) Start the CMP.
- 5) Click on the **Inventory** menu item on the **Maintenance** navigation tab of the CMP.
- 6) In the navigation tree, click on **Nodes**.
You see all nodes that are available in the OpenScape system.
- 7) Click on the name of the OpenScape 4000 system you have upgraded.
- 8) Select under **This node is:** the **self managed – version 7 or higher** option.
- 9) Specify port number **443** under **Administration Port**.
- 10) Click on **Save** to copy the settings.

The settings for the OpenScape 4000 node are saved and displayed in the node list.

10 Configuring a Certificate Strategy

IMPORTANT: Incorrect modifications of the certificates of the UC Application environment may enable unauthorized persons to access components and data of the system components involved.

IMPORTANT: During the following certificate strategy configuration, keys and certificates are copied to the computer systems of the UC Application environment. After you have successfully imported such keys and certificates in the keystore of the respective computer system you need to archive the kept keys and certificate files in a save location and delete them completely from the original computer system. This is the only way to prevent unauthorized persons from accessing confidential private keys, thus compromising the associated certificates.

NOTICE: All information about Large Deployment apply likewise for Very Large Deployment except as otherwise described.

The OpenScape system uses different security protocols.

- TLS / SSL – e. g. for the communication between different UC Application computer systems
- HTTPS – for the communication via a number of web-based interfaces.

You need to configure a certificate strategy for the smooth, secured communication via these protocols. The OpenScape system then integrates this strategy in the security concept of the customer network. How to proceed depends on two factors:

- The OpenScape deployment scenario used and its execution
- The available customer environment

10.1 Dependencies as regards the OpenScape Deployment Scenario

How you integrate the OpenScape system in the security concept of the customer network depends, among other things, on the OpenScape deployment scenario and its execution.

You need to differentiate the following scenarios:

- [Deployment scenario Integrated Deployment](#)
- [Deployment scenario Small Deployment](#)
- [Deployment scenario Large Deployment \(one front-end computer\)](#)
- [Deployment scenario Large Deployment \(several front-end computers\)](#)

Deployment scenario Integrated Deployment

In this deployment scenario the following UC Application computer systems must be integrated in the security concept of the customer network.

- The application computer
- The Facade server (if available)

NOTICE: Furthermore, you can configure individual certificates for an Openfire server possibly used. How to proceed is described in [Changing the Openfire Server Certificates](#) on page 505.

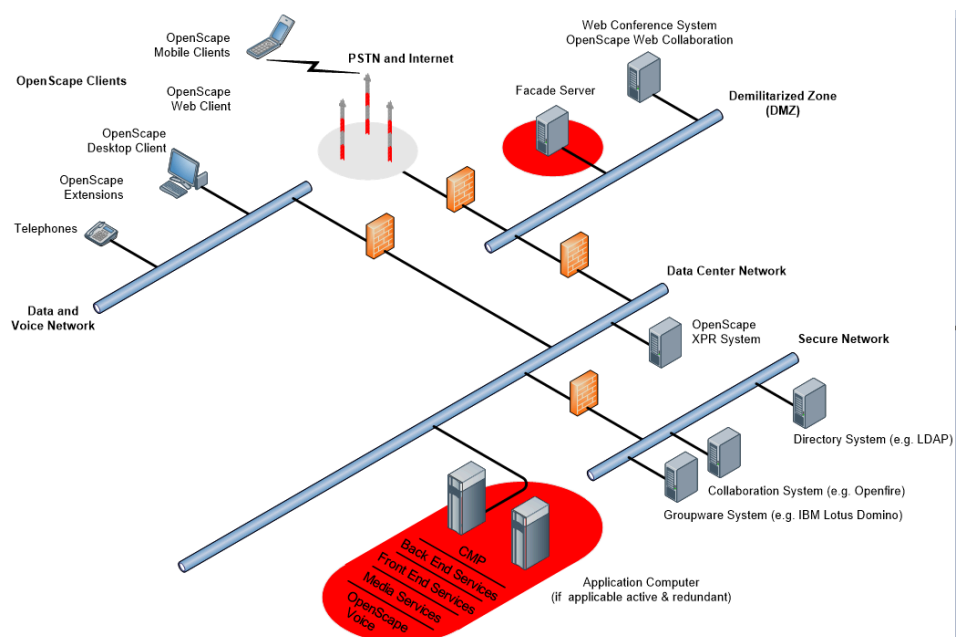
This integration requires altogether two pairs of key pair and certificate.

The key / certificate pair of the application computer must be assigned to the application computer. To this, the fully qualified host name (FQHN) of the application computer is specified in the certificate. The key / certificate pair is imported in the keystore of the application computer.

The key / certificate pair of the Facade server must have been assigned on the computer system of the Facade server. To this, the fully qualified host name (FQHN) of the Facade server computer is specified in the certificate. The key / certificate pair is imported in the keystore of the Facade server computer.

UC Application computer system to be integrated	Count Key pair / certificate	Certificate assigned to ...	Keystore storage location
Application computer	1	Application computer	Application computer
Facade server computer	1	Facade server computer	Facade server computer

The following figure shows the deployment scenario Integrated Deployment. All components concerned by the configuration of the certificate strategy in this scenario are red-highlighted.



Deployment scenario Small Deployment

In this deployment scenario the following UC Application computer systems must be integrated in the security concept of the customer network.

Configuring a Certificate Strategy

- The active application computer
- The passive application computer (if available)
- The Facade server (if available)

NOTICE: Furthermore, you can configure individual certificates for an Openfire server possibly used. How to proceed is described in [Changing the Openfire Server Certificates](#) on page 505.

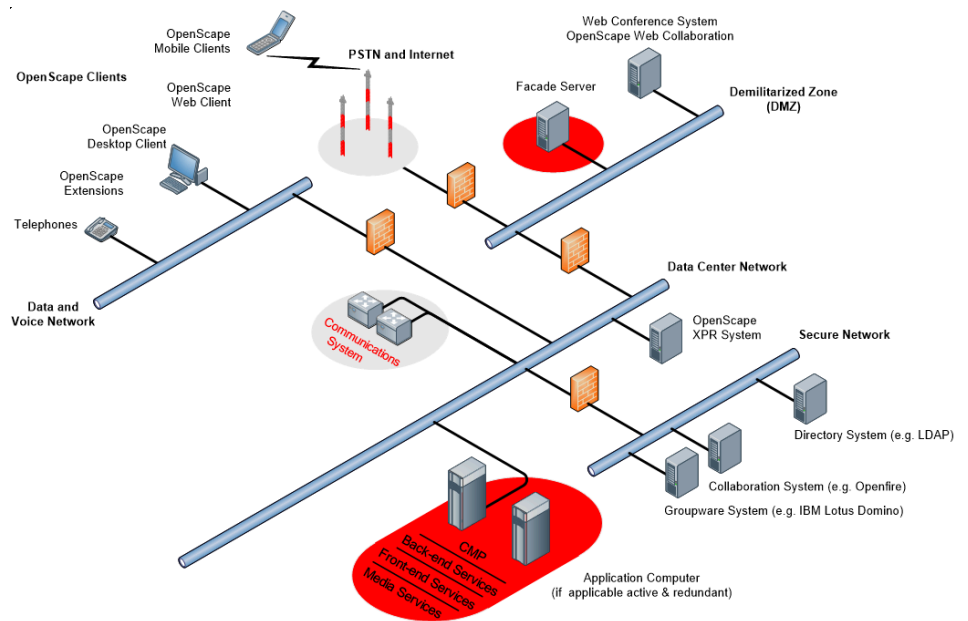
This integration requires altogether two pairs of key pair and certificate. The active and passive application computer use the same key / certificate pair, since these computer systems are addressed under the same host name.

The key / certificate pair of the application computer must be assigned to the application computers. To this, the fully qualified host name (FQHN) of the application computers is specified in the certificate. The key / certificate pair is imported in the keystore of the active and passive application computer.

The key / certificate pair of the Facade server must have been assigned on the computer system of the Facade server. To this, the fully qualified host name (FQHN) of the Facade server computer is specified in the certificate. The key / certificate pair is imported in the keystore of the Facade server computer.

UC Application computer system to be integrated	Count Key pair / certificate	Certificate assigned to ...	Keystore storage location
Application computer (active)	1	Application computer	Active application computer
Application computer (passive) (optional)			Passive application computer
Facade server computer	1	Facade server computer	Facade server computer

The following figure shows Small Deployment. All components concerned by the configuration of the certificate strategy in this deployment scenario are red-highlighted.



Deployment scenario Large Deployment (one front-end computer)

In this deployment scenario the following UC Application computer systems must be integrated in the security concept of the customer network.

- The active application computer
- The passive application computer
- The frontend computer
- The Facade server (if available)

NOTICE: Furthermore, you can configure individual certificates for the OpenScape Media Servers and an Openfire server possibly used. How to proceed is outlined in the manual *OpenScape Media Server, Administrator Documentation* or [Changing the Openfire Server Certificates](#) on page 505.

This integration requires altogether three pairs of key pair and certificate. The active and passive application computer use the same key / certificate pair, since these computer systems are addressed under the same host name.

The key / certificate pair of the application computer must be assigned to the application computers. To this, the fully qualified host name (FQHN) of the application computers is specified in the certificate. The key / certificate pair is imported in the keystore of the active and passive application computer.

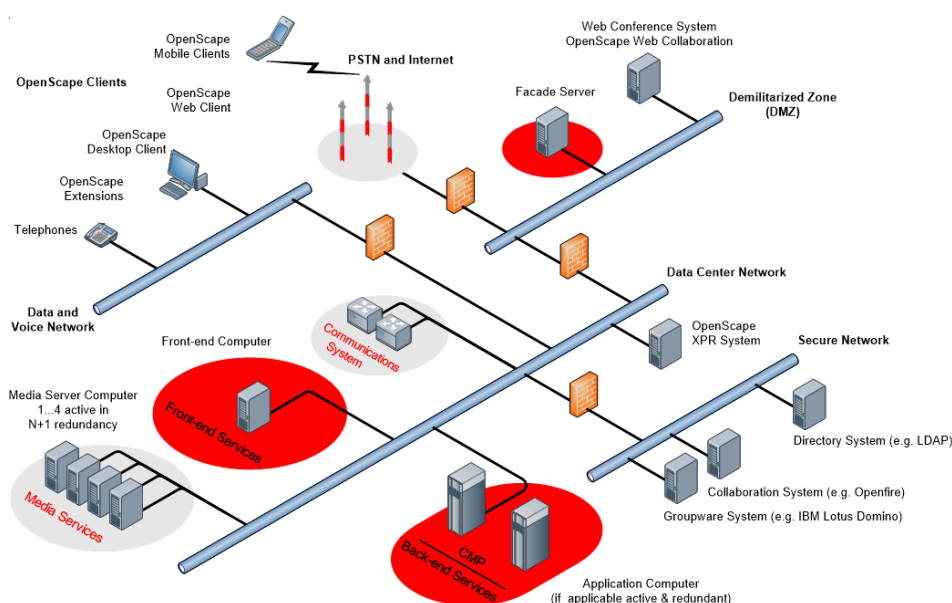
The key / certificate pair of the frontend computer must be assigned to the frontend computer. To this, the fully qualified host name (FQHN) of the frontend computer is specified in the certificate. The key / certificate pair is imported in the keystore of the frontend computer, but the keystore is administered on both application computers.

The key / certificate pair of the Facade server must have been assigned on the computer system of the Facade server. To this, the fully qualified host name (FQHN) of the Facade server computer is specified in the certificate. The key / certificate pair is imported in the keystore of the Facade server computer.

Configuring a Certificate Strategy

UC Application computer system to be integrated	Count Key pair / certificate	Certificate assigned to ...	Keystore storage location
Application computer (active)	1	Application computer	Active application computer
Application computer (passive)			Passive application computer
Front-end computer	1	Front-end computer	Active and passive application computer
Facade server computer	1	Facade server computer	Facade server computer

The following figure shows Large Deployment. All components concerned by the configuration of the certificate strategy in this deployment scenario are red-highlighted.



Deployment scenario Large Deployment (several front-end computers)

In this scenario the following UC Application computer systems must be integrated in the security concept of the customer network.

- The active application computer
- The passive application computer
- The various frontend computers
- The Facade server (if available)

NOTICE: Furthermore, you can configure individual certificates for the OpenScape Media Servers and an Openfire server possibly used. How to proceed is outlined in the manual *OpenScape Media Server, Administrator Documentation* or [Changing the Openfire Server Certificates](#) on page 505.

This integration requires altogether three pairs of key pair and certificate, for:

- The active and passive application computer use the same key / certificate pair, since these computer systems are addressed under the same host name.
- All frontend computers use the same key / certificate pair.
- The Facade server computer uses its own key / certificate pair.

The key / certificate pair of the application computer must be assigned to the application computers. To this, the fully qualified host name (FQHN) of the application computers is specified in the certificate. The key / certificate pair is imported in the keystore of the active and passive application computer.

The key / certificate pair of the frontend computers must be assigned to the load balancer system used. To this, the fully qualified host name (FQHN) of the load balancer system is specified in the certificate. The key / certificate pair is imported in the keystore of the frontend computers, but the keystore is administered on both application computers.

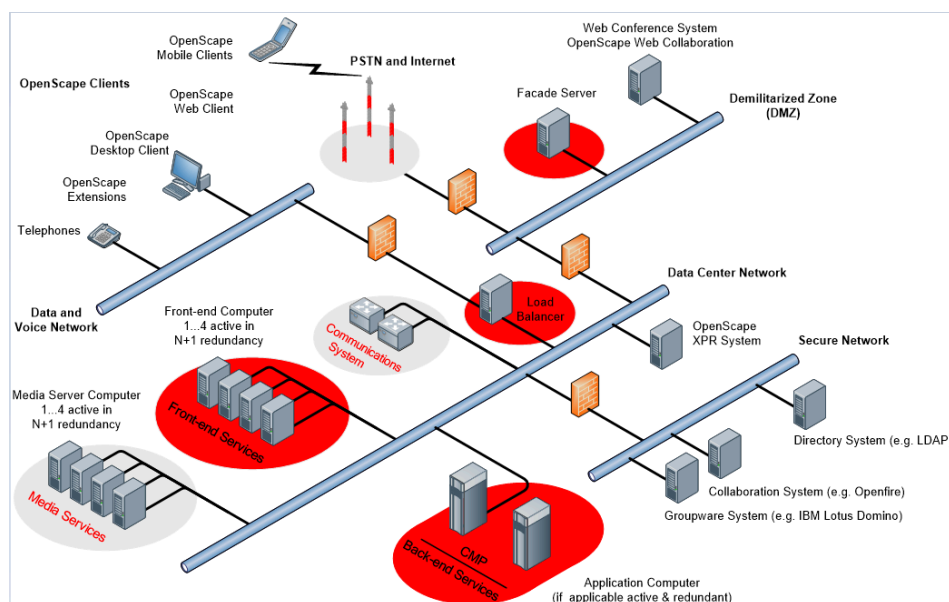
The key / certificate pair of the Facade server must have been assigned on the computer system of the Facade server. To this, the fully qualified host name (FQHN) of the Facade server computer is specified in the certificate. The key / certificate pair is imported in the keystore of the Facade server computer.

UC Application computer system to be integrated	Count Key pair / certificate	Certificate assigned to ...	Keystore storage location
Application computer (active)	1	Application computer	Active application computer
Application computer (passive)			Passive application computer
Frontend computer 1	1	Load balancer system	Active and passive application computer
Frontend computer 2			
Frontend computer 3 (optional)			
Frontend computer 4 (optional)			
Facade server computer	1	Facade server computer	Facade server computer

The following figure shows Large Deployment. All components concerned by the configuration of the certificate strategy in this deployment scenario are red-highlighted.

Configuring a Certificate Strategy

Contemplated Customer Environments



10.2 Contemplated Customer Environments

How you integrate the OpenScale system in the security concept of the customer network depends, among other things, on the available customer environment. The following description looks at the below customer environments and at the required configuration steps.

- [Customer Environment 1 \(CE 1\) – PKI with CA](#)
- [Customer Environment 2 \(CE 2\) – PKI with CA and CSR](#)
- [Customer Environment 3 \(CE 3\) – PKI without CA](#)
- [Customer Environment 4 \(CE 4\) – PKI planned](#)

The following sections describe the contemplated customer environments in detail.

10.2.1 Customer Environment 1 (CE 1) – PKI with CA

The customer network uses already a Public Key Infrastructure (PKI) with a proprietary Certificate Authority (CA). The customer provides required keys and associated certificates directly as PKCS#12 keystore file.

NOTICE: Which and how many key / certificate pairs are required for configuring the certificate strategy is outlined in [Dependencies as regards the OpenScale Deployment Scenario](#) on page 646.

The following requirements apply:

- The password for a PKCS#12 keystore file may contain the following characters only:
 - Letters A to Z and a to z
 - Digits 0 to 9
 - The special characters !\$() * + , - . / : ; = ? @ [\] ^ _ ` { | } ~
- The password for a PKCS#12 keystore file and the associated private key must be the same
- The password for a PKCS#12 keystore file must be known for the configuration
- The alias name **tomcat** must have been configured for the certificate in a PKCS#12 keystore file.
- The root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

Beyond that, the following recommendations apply:

- Private keys should be of type RSA
- The length of the keys used should be 2048 bit (the key lengths 1024 and 4096 are supported also)
- The signing algorithm should be MD5withRSA.

10.2.2 Customer Environment 2 (CE 2) – PKI with CA and CSR

The customer network uses already a Public Key Infrastructure (PKI) with a proprietary Certificate Authority (CA). A Certificate Sign Request (CSR) is required to provide required certificates.

The root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

10.2.3 Customer Environment 3 (CE 3) – PKI without CA

The customer already uses a public key infrastructure without proprietary certificate authority.

The root certificate of the certificate authority used has already been imported in the client browsers of the OpenScape users.

10.2.4 Customer Environment 4 (CE 4) – PKI planned

The customer has not used a public key infrastructure so far, but plans to introduce one with the OpenScape system.

10.3 Overview of the Configuration Steps

To configure the certificate strategy in one of the contemplated customer environments, you only need to execute the configuration steps marked with a check box for the relevant customer environment.

Configuration step	Customer environment:	CE 1	CE 2	CE 3	CE 4

Configuring a Certificate Strategy

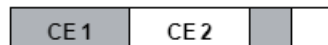
Preparing the Configuration of the Certificate Strategy				
• Determining the OpenScape Setup Directory	☐	☐	☐	☐
• Determining the Keytool Command	☐	☐	☐	☐
• Determining the Keystore Directory	☐	☐	☐	☐
• Determining the Directory for the SSL / TLS Configuration	☐	☐	☐	☐
• Defining an X.500 Distinguished Name		☐	☐	☐
Configuring a simple Certificate Authority				
• Preparing the Certificate Authority				☐
• Creating self-signed Root Certificates				☐
Creating a Pair of Keys for the Application Computer		☐	☐	☐
Creating Certificate Sign Requests for the Application Computer		☐	☐	☐
For Large Deployment: Creating a Pair of Keys for the Frontend Computer		☐	☐	☐
For Large Deployment: Creating a Certificate Sign Request for the Frontend Computer		☐	☐	☐
If OpenScape Mobile Clients are used: Creating a Pair of Keys for the Facade Server		☐	☐	☐
If OpenScape Mobile Clients are used: Creating a Certificate Sign Request for the Facade Server		☐	☐	☐
Signing Certificate Sign Requests		☐	☐	☐
Importing a Certificate in the Server Keystore		☐	☐	☐
Storing a provided PKCS#12 File	☐			
Activating a Server Keystore for the CMP	☐	☐	☐	☐
Configuring a Server Keystore for the Application Computer	☐	☐	☐	☐
Configuring Certificate and Keys for the BCom Component	☐	☐	☐	☐
For Large Deployment: Configuring a Server Keystore for the Multi-Node System	☐	☐	☐	☐
If OpenScape Mobile Clients are used: Configuring a Server Keystore for the Facade Server	☐	☐	☐	☐

Importing the Root Certificate in the Client Browsers					
	• Displaying the Root Certificate				☐
	• Checking the Root Certificate				☐
	• Installing the Root Certificate				☐
If OpenScape Mobile Clients are used: Importing the Root Certificate in the Mobile Phones					☐
If the SPML⁹² interface is used: Configuring the Certificate for the SPML Interface		☐	☐	☐	☐
If the OpenScape UC Graph Connector is used: Configuring the Certificate for the UC Graph Connector					

A graphic representation shows you in every configuration chapter of for which of these customer environments you need to execute the relevant configuration steps.

Example:

Execute these steps for:



You need to execute the configuration steps of the relevant configuration chapter for customer environments 1 and 2 only.

[Supplementing Instructions](#) on page 687 contains the following instructions in addition. You may need these instructions to configure the certificate strategy in a customer environment.

- [Creating a secure Password](#)
- [Combining Certificate Files to a Certificate Chain](#)
- [Converting the Format of a Certificate Chain from DER into PEM](#)
- [Converting the Format of a Certificate Chain from PKCS#12 into PEM](#)

10.4 Preparing the Configuration of the Certificate Strategy

You need to execute the following preparatory steps before you can configure the certificate strategy.

- [Determining the OpenScape Setup Directory](#)
- [Determining the Keytool Command](#)
- [Determining the Keystore Directory](#)
- [Determining the Directory for the SSL / TLS Configuration](#)
- [Defining an X.500 Distinguished Name](#)

These steps are described in detail in the following sections.

⁹² The SPML interface provides an SOAP-based access to the OpenScape UC Application features.

10.4.1 Determining the OpenScape Setup Directory

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

To configure a computer system for the certificate strategy you need to know the directory in which OpenScape UC Application was installed on the computer system.

You need this information for the following UC Application computer systems:

- For an application computer
- For a frontend computer (if available)

Start the configuration

How to determine the setup directory of OpenScape UC Application for an UC Application computer system:

- 1) Open a shell on the relevant computer system and log on as root user.
- 2) Execute the following command:

```
cat /etc/sysconfig/siemens/symphonia
```

In the system output the SYMPHONIA_HOME parameter specifies the OpenScape UC Application setup directory.

Example: SYMPHONIA_HOME=/opt/siemens

- 3) Determine the OpenScape UC Application setup directory for each of the described UC Application computer systems.

In the following configuration steps we generally name an OpenScape UC Application setup directory: *<SymphoniaHome>*

To document the determined setup directories:

	Application computer	Front-end computer
<i><SymphoniaHome></i>		

10.4.2 Determining the Keytool Command

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

Configuring the certificate strategy requires the `keytool` command, which belongs to the Java Runtime Environment (JRE) of OpenScape UC Application. You need to determine how to invoke this command.

You need this information for the following UC Application computer systems:

- For an application computer
- For a frontend computer (if available)
- For the computer system of the Facade server (if available)

Start the configuration

How to determine the correct `keytool` command for an UC Application computer system:

- 1) Open a shell on the relevant computer system and log on as root user.
- 2) Execute the following command:

```
cat /etc/sysconfig/siemens/symphonia
```

In the system output the `SYMPHONIA_JAVA` parameter specifies the first part of the directory path that leads to the correct `keytool` command.

Example: `SYMPHONIA_JAVA=/opt/siemens/share/ibm-java2-i386-60/jre`

- 3) Attach the following directories to the determined first part of the directory path to receive the complete directory path for the `keytool` command:

```
/bin/keytool
```

Example: `/opt/siemens/share/ibm-java2-i386-60/jre/bin/keytool`

- 4) Determine the `keytool` command for each of the described UC Application computer systems.

Using the following command you can create an alias for the correct `keytool` command:

```
alias keytool=<complete directory path>
```

You can now invoke the correct `keytool` command in the shell by simply specifying the `keytool` command.

NOTICE: The alias is valid until you close the shell.

10.4.3 Determining the Keystore Directory

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

Keystores, certificates and keys must be stored on the UC Application computer systems in a specific directory. You need to determine this directory.

You need this information for the following UC Application computer systems:

- For an application computer
- For a frontend computer (if available)

Start the configuration

How to determine the directory for storing keystores, certificates and keys for an UC Application computer system:

- 1) Open a shell on the relevant computer system and log on as root user.
- 2) Execute the following command:

```
(. /etc/sysconfig/siemens/ca;echo "$CA_DIST")
```

The relevant directory is put out in the shell.

Example: `/opt/siemens/HiPathCA/distribution`

- 3) Determine the keystore directory for each of the described UC Application computer systems.

In the following configuration steps we generally name a keystore directory: *<CaDistribution>*

To document the determined keystore directories:

	Application computer	Front-end computer
<i><CaDistribution></i>		

10.4.4 Determining the Directory for the SSL / TLS Configuration

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

OpenScape UC Application uses different SSL and TLS configuration files that must be stored in a specific directory on the UC Application computer systems. You need to determine this directory.

You need this information for the following UC Application computer systems:

- For an application computer
- For a frontend computer (if available)

Start the configuration

How to determine the directory in which the SSL and TLS configuration files are stored for an UC Application computer system:

- 1) Open a shell on the relevant computer system and log on as root user.
- 2) Execute the following command in one line:

```
(. /etc/sysconfig/siemens/ca; echo "$CA_CONFIG_ROOT/services/default/Httpd")
```

The relevant directory is put out in the shell.

Example: /opt/siemens/HiPathCA/config/services/default/Httpd

- 3) Determine the configuration file directory for each of the described UC Application computer systems.

In the following configuration steps we generally name a configuration file directory: *<CaConfigHttpd>*

To document the determined configuration file directories:

	Application computer	Front-end computer
<i><CaConfigHttpd></i>		

10.4.5 Defining an X.500 Distinguished Name

Execute these steps for:

	CE 2	CE 3	CE 4

To define the assignment of certificates or keys to computer systems, a unique name – the so-called Distinguished Name (DN) – is specified in each certificate or key.

The distinguished name contains the following information that should always be defined.

- **CN** – Common Name

Must as a rule define the Fully Qualified Host Name (FQHN) of the computer system to which the certificate and the associated pair of keys are assigned.

Example: filesrv_ac1.domain.com

In case of a Certificate Authority (CA), CN must define the name of the certificate authority.

Example: RWTH Aachen Intermediate CA

- **OU** – Organization Unit

Must define the name of a smaller organization unit the relevant computer system belongs to – e. g. a department or division.

Example: University library

Furthermore, the distinguished name contains the following information that can be defined in addition.

- **O** – Organization Name

May define the name of a larger organization unit the relevant computer system belongs to.

Example: RWTH Aachen

- **L** – Locality

May define the geographic location for the relevant computer system – e. g. the name of a city.

Example: Aachen

- **C** – Country

May define the two-digit country code for the location of the relevant computer system.

Example: DE

- **ST** – State Name

May define the name of a subordinate territory for the location of the relevant computer system.

Example: NRW

NOTICE: Instead of the **ST** identifier the Java keytool uses the **S** identifier.

NOTICE: An existing customer environment uses in most cases already defined information for setting up a distinguished name.

Example of a distinguished name as you need to enter it in commands of the Java keytool at a later date: CN=filesrv_ac1.domain.com, OU=University library, O=RWTH Aachen, L=Aachen, C=DE, S=NRW

Define a distinguished name for the following UC Application computer systems. The values for OU, O, L, C, and ST (S) are identical for all systems.

	CN (FQHN)	ou (Org-Unit)	O (Org-Name)	L (Locality)	C (Country)	ST (S) (State)
Application computer	93					
Front-end computer or Load balancer system (if available)	94					
Facade server computer (if available)						

In the following configuration steps we generally name a distinguished name: *<DistinguishedName>*

You have now completed all preparatory steps for configuring the certificate strategy.

⁹³ If an active and passive application computer are available, both computer systems are addressed under the same host name.

⁹⁴ If only a single frontend computer is used, CN is for the associated certificate the Fully Qualified Host Name (FQHN) of this frontend computer. If several frontend computer are used, CN is for the associated certificate the fully qualified host name of the load balancer system used. All frontend computers use the same certificate and thus the same pair of keys in this case.

10.5 Configuring a simple Certificate Authority

Execute these steps for:



The following steps configure a simple certificate authority on one of the application computer of OpenScape UC Application. The freely available software *OpenSSL*⁹⁵ is used for this purpose. This software is usually pre-installed with each Linux operating system.

The certificate authority configured in this way should only be used for testing purposes. This is because:

- A certificate authority should always be configured and operated on a separate computer system.
- Passwords should not be transferred via a command console.
- The random generator used in the following should better be pre-set for a certificate authority.

The certificate authority is configured in the following steps.

- [Preparing the Certificate Authority](#)
- [Creating self-signed Root Certificates](#)

10.5.1 Preparing the Certificate Authority

Execute these steps for:



The certificate authority is configured on an application computer of OpenScape UC Application. This requires creating a working directory for the certificate authority on the application computer – e. g. the following OpenScape UC Application setup directory:

`<SymphoniaHome>/common/conf/ca`

Various files of the certificate authority are stored in this working directory.

In the following configuration steps we generally name the directory path just created for the working directory of the certificate authority as follows:
`<CaBaseDir>`

Start the configuration

How to create the new working directory `<CaBaseDir>` on the application computer of OpenScape UC Application for the certificate authority:

- 1) Open a shell on the relevant application computer and log on as root user.
- 2) Execute the following command to create the new working directory if it does not exist yet:

```
test -d <CaBaseDir> || mkdir -p <CaBaseDir>
```

⁹⁵ You find further information about the software OpenSSL under: <http://www.openssl.org/>

- 3) Execute the following command to grant exclusively the root user all privileges for the new working directory.

```
chmod 700 <CaBaseDir>
```

- 4) Start a text editor and open the following file therein:

```
<CaBaseDir>/openssl.cnf.
```

- 5) Enter the following text in the new file. Use the individual data of your current system environment for the bolded entries.

```
ca_base_dir=<CaBaseDir>
RANDFILE=$ENV::HOME/.rnd

[ ca ]
default_ca=CA_local

[ CA_local ]
dir=<CaBaseDir>
certs=$dir
new_certs_dir=$dir/ca_certs.d
database=$dir/ca.db.index
serial=$dir/ca.db.serial
certificate=$dir/ca_root.pem
private_key=$dir/private/ca_root.key
x509_extensions=v3_sign
default_days=3652
default_crl_days=30
default_md=md5
preserve=no
policy=policy_anything

[ policy_anything ]
countryName=optional
stateOrProvinceName=optional
localityName=optional
organizationName=optional
organizationalUnitName=optional
commonName=optional
emailAddress=optional

[ req ]
prompt=no
default_bits=2048
distinguished_name=req_distinguished_name
x509_extensions=v3_ca

[ req_distinguished_name ]
CN=Local CA OU=<OU>96
O=<O>96
L=<L>96
C=<C>96
ST=<ST>96
```

⁹⁶ You have already defined the value for this entry in [Defining an X.500 Distinguished Name](#) on page 658.

```
[ v3_sign ]
basicConstraints=CA:FALSE
nsComment="OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer

[ v3_ca ]
basicConstraints=critical, CA:TRUE
keyUsage=cRLSign, keyCertSign
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
```

- 6) Save the modifications in the file `<CaBaseDir>/openssl.cnf`.
- 7) Execute the following command to switch to the working directory of the certificate authority.

```
cd <CaBaseDir>
```

- 8) Execute the following commands to create further directories and files required by the certificate authority.

```
test -d "private" || mkdir "private"
test -d "ca_certs.d" || mkdir "ca_certs.d"
test -f "ca.db.index" || touch ca.db.index
test -f "ca.db.serial" || echo "01" > "ca.db.serial"
```

- 9) Execute the following commands to exclusively grant the root user all privileges for the new directories and files.

```
chmod 700 "private" "ca_certs.d"
chmod 600 "openssl.cnf" "ca.db.index" "ca.db.serial"
```

10.5.2 Creating self-signed Root Certificates

Execute these steps for:



A signed root certificate of the certificate authority is required to have individual keys signed by the certificate authority at a later date.

Start the configuration

How to create a self-signed root certificate for the certificate authority:

- 1) Create a password that you use immediately for creating the root certificate. Use the procedure from e. g. [Creating a secure Password](#) on page 687 for this purpose.

In the following configuration steps we name this password:
`<CaKeyPassword>`

- 2) Open a shell on the application computer on which the certificate authority has been prepared and log on as root user.
- 3) Execute the following command to switch to the working directory of the certificate authority.

```
cd <CaBaseDir>
```

- 4) Execute the following command in one line to create a pair of keys that contains a private and a public key.

```
openssl genrsa
-rand "$HOME/.rnd"
-out private/ca_root.key
-des3
-passout 'pass:<CaKeyPassword>' 2048
```

The newly created pair of keys is stored under the name `ca_root.key` in the directory `<CaBaseDir>/private`.

- 5) Execute the following command in one line to create a root certificate signed with the just created private key.

```
openssl req
-config openssl.cnf
-x509
-md5
-days 3652
-new
-key private/ca_root.key
-passin 'pass:<CaKeyPassword>'
-out ca_root.pem
```

The newly created root certificate is valid for 10 years (3652 days). It is stored under the name `ca_root.pem` in the directory `<CaBaseDir>`.

- 6) Execute the following command in one line to convert the just created root certificate in the DER format.

```
openssl x509
-outform DER
-in ca_root.pem
-out ca_root.der
```

The newly formatted root certificate is stored under the name `ca_root.der` in the directory `<CaBaseDir>`.

- 7) Execute the following commands to exclusively grant the root user all privileges for the pair of keys and the root certificates.

```
chmod 600 "private/ca_root.key"
chmod 600 "ca_root.pem" "ca_root.der"
```

- 8) Execute the following command to display the contents of the just created root certificate.

```
keytool -printcert -v -file ca_root.pem
```

The output has the following format:

```
Owner: ST=NRW, C=DE, L=Aachen, O=RWTH Aachen,
OU=University library, CN=Local CA
Issuer: ST=NRW, C=DE, L=Aachen, O=RWTH Aachen,
OU=University library, CN=Local CA
Serial number: 9c2dd539201cb111
Valid from: 7/15/09 11:02 AM until: 7/15/19 11:02 AM
Certificate fingerprints:
- MD5: 04:22:33:03:1A:27:99:62:8C:83:81:A0:A2:0A:C6:80
- SHA1:
58:E8:6E:58:19:B0:62:52:D0:4C:6B:E8:1D:34:C3:F2:6A:26:77:59
```

10.6 Creating a Pair of Keys for the Application Computer

Execute these steps for:

	CE 2	CE 3	CE 4

You need to create a pair of keys for the application computer. If you use an active and a passive application computer, both application computers use the same pair of keys, since these computer systems are addressed under the same host name.

The pair of keys of the application computer must be assigned to the application computer. When the pair of keys is created, the distinguished name of the application computer is specified for this assignment.

NOTICE: If you use an active and a passive application computer, you need to execute the following steps on one of the application computers only.

Start the configuration

How to create a pair of keys on the application computer:

- 1) Create a password that you use immediately for creating the pair of keys. Use the procedure from e. g. [Creating a secure Password](#) on page 687 for this purpose.

This password is used to protect the keystore and the pair of keys contained therein from unauthorized access.

In the following configuration steps we name this password: *<Key/StorePassword>*

NOTICE: Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access, the password should be generated randomly. Each pair of keys of a keystore can also be protected from unauthorized access by a key password. This key password, however, must usually correspond to the keystore password.

- 2) Open a shell on the application computer on which the certificate authority has been configured and log on as root user.
- 3) Execute the following command:

```
cd <SymphoniaHome>/common/conf
```
- 4) Execute the following command in one line to create a pair of keys that contains a private and a public key.

```
keytool -genkey  
-keystore keystore.p12  
-storetype pkcs12  
-storepass '<Key/StorePassword>'  
-keyalg RSA  
-keysize 2048  
-validity 3652
```

Configuring a Certificate Strategy

Creating Certificate Sign Requests for the Application Computer

```
-dname '<DistinguishedName97> '  
-keypass '<Key/StorePassword> '  
-alias AppServer
```

The newly created pair of keys is stored under the alias AppServer in the likewise newly created keystore keystore.p12. The newly created pair of keys is valid for 10 years (3652 days).

NOTICE: The maximum permissible validity of a pair of keys can be restricted in an existing customer environment. In this case, adjust the value for the -validity option accordingly.

NOTICE: Creating a pair of key may take some minutes.

10.7 Creating Certificate Sign Requests for the Application Computer

Execute these steps for:

	CE 2	CE 3	CE 4

The newly created pair of keys for the application computer must be signed by a certificate authority. To this, a Certificate Sign Request (CSR) must be created for this pair of keys.

Start the configuration

How to create a certificate sign request for the pair of keys of an application computer:

- 1) Open a shell on the application computer on which you have created the pair of keys and log on as root user.
- 2) Execute the following command:

```
cd <SymphoniaHome>/common/conf
```

- 3) Execute the following command in one line to create a certificate sign request for the pair of keys of the application computer.

```
keytool -certreq  
-keystore keystore.p12  
-storetype pkcs12  
-storepass '<Key/StorePassword> '  
-alias AppServer  
-file tomcat_csr.pem
```

The newly created certificate sign request is stored under the name tomcat_csr.pem in the current directory.

⁹⁷ You have already defined the distinguished name for the application computer in [Defining an X.500 Distinguished Name](#) on page 658. The following example shows the entry format for this value: CN=filesrv_ac1.domain.com, OU=Universitaetsbibliothek, O=RWTH Aachen, L=Aachen, C=DE, S=NRW *IMPORTANT:* Please note that you need to enter the commas and blanks, too.

- 4) Execute the following command to display the contents of the just created certificate sign request.

```
openssl req -in tomcat_csr.pem -text -noout
```

The created Certificate Sign Request will be signed in later configuration step by the certificate authority.

10.8 Creating a Pair of Keys for the Frontend Computer

Execute these steps for:

	CE 2	CE 3	CE 4

NOTICE: You need to execute the following steps for Large Deployment only.

You need to create a pair of keys for the frontend computer. If you deploy several frontend computers, they all use the same pair of keys.

The pair of keys of the frontend computers must be assigned to one of the following computer systems.

- If you use only one frontend computer, the pair of keys must be assigned to this frontend computer
- If you use several frontend computers, the pair of keys must be assigned to the load balancer system used.

When the pair of keys is created, the distinguished name of the relevant computer system is specified for this assignment.

NOTICE: If you use several frontend computers, you need to execute the following steps on only one of the frontend computers used.

Start the configuration

How to create a pair of keys on the frontend computer:

- 1) Create a password that you use immediately for creating the pair of keys. Use the procedure from e. g. [Creating a secure Password](#) on page 687 for this purpose.

This password is used to protect the keystore and the pair of keys contained therein from unauthorized access.

In the following configuration steps we name this password: *<Key/StorePassword>*

NOTICE: Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access, the password should be generated randomly. Each pair of keys of a keystore can also be protected from unauthorized access by a key

Configuring a Certificate Strategy

Creating a Certificate Sign Request for the Frontend Computer

password. This key password, however, must usually correspond to the keystore password.

2) Open a shell on the frontend computer and log on as root user.

3) Execute the following command:

```
cd <SymphoniaHome>/common/conf
```

Execute the following command in one line to create a pair of keys that contains a private and a public key.

```
keytool -genkey
-keystore keystore.p12
-storetype pkcs12
-storepass '<Key/StorePassword>'
-keyalg RSA
-keysize 2048
-validity 3652
-dname '<DistinguishedName98>'
-keypass '<Key/StorePassword>'
-alias FEServer
```

The newly created pair of keys is stored under the alias FEServer in the likewise newly created keystore keystore.p12. The newly created pair of keys is valid for 10 years (3652 days).

NOTICE: The maximum permissible validity of a pair of keys can be restricted in an existing customer environment. In this case, adjust the value for the -validity option accordingly.

NOTICE: Creating a pair of key may take some minutes.

10.9 Creating a Certificate Sign Request for the Frontend Computer

Execute these steps for:

	CE 2	CE 3	CE 4

NOTICE: You need to execute the following steps for Large Deployment only.

The newly created pair of keys for the frontend computer must be signed by a certificate authority. To this, a Certificate Sign Request (CSR) must be created for this pair of keys.

⁹⁸ You have already defined the distinguished name for the pair of keys of the frontend computer in [Defining an X.500 Distinguished Name](#) on page 658. The following example shows the entry format for this value: CN=filesrv_ac1.domain.com, OU=Universitaetsbibliothek, O=RWTH Aachen, L=Aachen, C=DE, S=NRW **IMPORTANT:** Please note that you need to enter the commas and blanks, too.

Start the configuration

How to create a certificate sign request for the pair of keys of the frontend computer:

- 1) Open a shell on the frontend computer on which you have created the pair of keys and log on as root user.
- 2) Execute the following command:
`cd <SymphoniaHome>/common/conf`
- 3) Execute the following command in one line to create a certificate sign request for the pair of keys of the frontend computer.

```
keytool -certreq  
-keystore keystore.p12  
-storetype pkcs12  
-storepass '<Key/StorePassword>'  
-alias FEServer  
-file tomcat_csr.pem
```

The newly created certificate sign request is stored under the name `tomcat_csr.pem` in the current directory.

- 4) Execute the following command to display the contents of the just created certificate sign request.

```
openssl req -in tomcat_csr.pem -text -noout
```

The created Certificate Sign Request will be signed in later configuration step by the certificate authority.

10.10 Creating a Pair of Keys for the Facade Server

Execute these steps for:

	CE 2	CE 3	CE 4

NOTICE: You need to execute the following steps only if you use the OpenScape Mobile Client.

You need to create a pair of keys for the Facade server probably used.

The pair of keys of the Facade server must be assigned to the computer system of the Facade server. When the pair of keys is created, the distinguished name of the computer system on which the Facade server is installed is specified for this assignment.

Start the configuration

How to create a pair of keys on the computer system of the Facade server:

- 1) Create a password that you use immediately for creating the pair of keys. Use the procedure from e. g. [Creating a secure Password](#) on page 687 for this purpose.

This password is used to protect the keystore and the pair of keys contained therein from unauthorized access.

In the following configuration steps we name this password: `<Key/StorePassword>`

NOTICE: Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access, the password should be generated randomly. Each pair of keys of a keystore can also be protected from unauthorized access by a key password.

- 2) Open a shell on the computer system on which the Facade server is installed and log on as root user.
- 3) Execute the following command:

```
cd /usr/local/tomcat6/conf
```
- 4) Execute the following command in one line to create a pair of keys that contains a private and a public key.

```
keytool -genkey
-keystore keystore.p12
-storetype pkcs12
-storepass '<Key/StorePassword>'
-keyalg RSA
-keysize 2048
-validity 3652
-dname '<DistinguishedName99>'
-keypass '<Key/StorePassword>'
```

⁹⁹ You have already defined the distinguished name for the application computer in [Defining an X.500 Distinguished Name](#) on page 658. The following example shows the entry format for this value: `CN=filesrv_ac1.domain.com, OU=Universitaetsbibliothek, O=RWTH Aachen, L=Aachen, C=DE, S=NRW` *IMPORTANT:* Please note that you need to enter the commas and blanks, too.

```
-alias Tomcat
```

The newly created pair of keys is stored under the alias `tomcat` in the likewise newly created keystore `keystore.p12`. The newly created pair of keys is valid for 10 years (3652 days).

IMPORTANT: Key and keystore password must be identical.

IMPORTANT: Always use the alias **tomcat** for the pair of keys of the Facade server.

NOTICE: The maximum permissible validity of a pair of keys can be restricted in an existing customer environment. In this case, adjust the value for the `-validity` option accordingly.

NOTICE: Creating a pair of key may take some minutes.

10.11 Creating a Certificate Sign Request for the Facade Server

Execute these steps for:

	CE 2	CE 3	CE 4

NOTICE: You need to execute the following steps only if you use the OpenScape Mobile Client.

The newly created pair of keys for the Facade server must be signed by a certificate authority. To this, a Certificate Sign Request (CSR) must be created for this pair of keys.

Start the configuration

How to create a certificate sign request for the pair of keys of the Facade server:

- 1) Open a shell on the computer system on which you have created the pair of keys and log on as root user.
- 2) Execute the following command:

```
cd /usr/local/tomcat6/conf
```
- 3) Execute the following command in one line to create a certificate sign request for the pair of keys of the Facade server:

```
keytool -certreq  
-keystore keystore.p12  
-storetype pkcs12  
-storepass '<Key/StorePassword>'  
-alias Tomcat
```

Configuring a Certificate Strategy

Signing Certificate Sign Requests

```
-file tomcat_csr.pem
```

The newly created certificate sign request is stored under the name `tomcat_csr.pem` in the current directory.

- 4) Execute the following command to display the contents of the just created certificate sign request.

```
openssl req -in tomcat_csr.pem -text -noout
```

The created Certificate Sign Request will be signed in later configuration step by the certificate authority.

10.12 Signing Certificate Sign Requests

Execute these steps for:

	CE 2	CE 3	CE 4

The newly created pairs of keys must be signed to confirm the identity of the associated computer systems. To this, the associated certificate sign requests are signed by a certificate authority. This results in certificates that contain the following:

- The public key of the relevant computer system
- Information that identifies the associated computer system
- General information about the certificate itself.

You can sign the certificate sign requests in two ways:

- By a certificate authority that you have configured in the scope of these instructions. In this case, proceed as documented for the relevant certificate authority, and skip the descriptions that follow in this section.
- By the certificate authority you have configured in [Configuring a simple Certificate Authority](#) on page 661. In this case, proceed as described in the following.

Start the configuration

How to sign the certificate sign request with the certificate authority from [Configuring a simple Certificate Authority](#) on page 661:

- 1) Open a shell on the application computer on which the certificate authority has been configured and log on as root user.
- 2) Copy the certificate sign request `tomcat_csr.pem` from the directory `<SymphoniaHome>/common/conf` to the following working directory of the certificate authority:

`<CaBaseDir>`

- 3) Execute the following command to switch to the working directory of the certificate authority.

```
cd <CaBaseDir>
```

- 4) Execute the following command in one line to sign the certificate sign request `tomcat_csr.pem` of the application computer with the root certificate of the certificate authority.

```
openssl ca  
-config openssl.cnf  
-days 3652
```

```
-passin 'pass:<CaKeyPassword>'
-notext
-batch
-in tomcat_csr.pem
-out tomcat_cert.pem
```

The newly created certificate is stored under the name `tomcat_cert.pem` in the working directory `<CaBaseDir>`. It is valid for 10 years (3652 days).

NOTICE: The maximum permissible validity of a certificate can be restricted in an existing customer environment. In this case, adjust the value for the `-days` option accordingly.

- 5) Move the certificate `tomcat_cert.pem` from the working folder `<CaBaseDir>` to the following directory:
`<SymphoniaHome>/common/conf`
- 6) Copy the certificate sign request `tomcat_csr.pem` from the directory `<SymphoniaHome>/common/conf` of the frontend computer to the following working directory of the certificate authority:
`<CaBaseDir>`
- 7) Execute steps 3 and 4 once more to sign the certificate sign request of the frontend computer.
- 8) Move the certificate `tomcat_cert.pem` from the working folder `<CaBaseDir>` to the following directory of the frontend computer on which you have created the pair of keys:
`<SymphoniaHome>/common/conf`
- 9) Copy the certificate sign request `tomcat_csr.pem` from the `/usr/local/tomcat6/conf` directory of the Facade server to the following working folder of the certificate authority:
`<CaBaseDir>`
- 10) Execute steps 3 and 4 once more to sign the certificate sign request of the Facade server.
- 11) Move the certificate `tomcat_cert.pem` from the working folder `<CaBaseDir>` to the following directory of the Facade server computer on which you have created the pair of keys:
`/usr/local/tomcat6/conf`

10.13 Importing a Certificate in the Server Keystore

Execute these steps for:

	CE 2	CE 3	CE 4

To enable the UC Application computer systems using their keys and associated signed certificates for communication, keys and signed certificates must be combined in the associated PKCS#12 file.

Start the configuration

How to store the newly created pairs of keys and associated certificates as PKCS#12 file in the associated keystore:

- 1) Open a shell on the application computer on which you have created the pair of keys and log on as root user.
- 2) Copy the root certificate `ca_root.pem` of the CA to the following directory of the application computer.

`<SymphoniaHome>/common/conf`

NOTICE: Further intermediate certificates may be required to ascertain the correctness of the certificate `tomcat_cert.pem`. In this case, use the file of the certificate chain of intermediate and root certificate instead of the simple root certificate `ca_root.pem`. How to combine several certificates to a certificate chain is described in [Combining Certificate Files to a Certificate Chain](#) on page 688.

- 3) Execute the following command:
`cd <SymphoniaHome>/common/conf`
- 4) Execute the following command in one line to create a PKCS#12 file that contains the pair of keys from the keystore.

```
openssl pkcs12
-in keystore.p12
-passin 'pass:<Key/StorePassword>'
-nocerts
-out keystore.pem
-passout 'pass:<Key/StorePassword>'
```

The pair of keys of keystore `keystore.p12` is stored in the local directory in the PKCS#12 file `keystore.pem`.

- 5) Execute the following command in one line to create a PKCS#12 keystore file that contains the pair of keys and all associated certificates.

```
openssl pkcs12
-export
-out tomcat-keystore.p12
-passout 'pass:<Key/StorePassword>'
-inkey keystore.pem
-passin 'pass:<Key/StorePassword>'
-in tomcat_cert.pem
-name tomcat
-certfile ca_root.pem
-caname root
```

NOTICE: Further intermediate certificates may be required to ascertain the correctness of the certificate `tomcat_cert.pem`. In this case, use the file of the certificate chain of intermediate and root certificate instead of the simple root certificate `ca_root.pem`. How to combine several certificates to a certificate chain is described in [Combining Certificate Files to a Certificate Chain](#) on page 688.

The pair of keys and all required certificates are stored in the local directory in the PKCS#12 keystore file `tomcat-keystore.p12`.

- 6) If you use an active and passive application computer: Copy the PKCS#12 keystore file `tomcat-keystore.p12` to the corresponding directory of the second application computer.
- 7) If you use Large Deployment: Execute steps 1 to 5 also on the frontend computer on which you have created the pair of keys.
- 8) If you use a Facade server, execute the following steps.
 - a) Open a shell on the Facade server computer on which you have created the pair of keys and log on as root user.
 - b) Copy the root certificate `ca_root.pem` of the CA to the following directory of the Facade server computer:

`/usr/local/tomcat6/conf`

NOTICE: Further intermediate certificates may be required to ascertain the correctness of the certificate `tomcat_cert.pem`. In this case, use the file of the certificate chain of intermediate and root certificate instead of the simple root certificate `ca_root.pem`. How to combine several certificates to a certificate chain is described in [Combining Certificate Files to a Certificate Chain](#) on page 688.

- c) Execute the following command:


```
cd /usr/local/tomcat6/conf
```
- d) Rename the following keystore file installed with the Facade server by default. In this way you can restore the default configuration at a later date if required.


```
OSC-Facade-Server-Default-Cert.p12
```
- e) Execute the following command in one line to create a PKCS#12 file that contains the new pair of keys from the keystore `keystore.p12`.

```
openssl pkcs12
-in keystore.p12
-passin 'pass:<Key/StorePassword>'
-nocerts
-out keystore.pem
-passout 'pass:<Key/StorePassword>'
```

The pair of keys of keystore `keystore.p12` is stored in the local directory in the PKCS#12 file `keystore.pem`.

- f) Execute the following command in one line to create under the default keystore name a PKCS#12 keystore file that contains the pair of keys and all associated certificates.

```
openssl pkcs12
-export
-out OSC-Facade-Server-Default-Cert.p12
-passout 'pass:<Key/StorePassword>'
-inkey keystore.pem
-passin 'pass:<Key/StorePassword>'
-in tomcat_cert.pem
-name tomcat
-certfile ca_root.pem
```

Configuring a Certificate Strategy

Storing a provided PKCS#12 File

-caname root

NOTICE: Further intermediate certificates may be required to ascertain the correctness of the certificate `tomcat_cert.pem`. In this case, use the file of the certificate chain of intermediate and root certificate instead of the simple root certificate `ca_root.pem`. How to combine several certificates to a certificate chain is described in [Combining Certificate Files to a Certificate Chain](#) on page 688.

The pair of keys and all required certificates are stored in the local directory in the following PKCS#12 keystore file: `OSC-Facade-Server-Default-Cert.p12`

10.14 Storing a provided PKCS#12 File

Execute these steps for:



NOTICE: Execute the steps of this section only if the required PKCS#12 keystore files have been provided to you so that you did not have to create them manually.

If prepared PKCS#12 files are provided for configuring the certificate strategy, you merely need to store these files on the associated UC Application computer systems.

NOTICE: How many PKCS#12 keystore files you require in total is a subject of [Dependencies as regards the OpenScape Deployment Scenario](#) on page 646.

Start the configuration

How to store the provided PKCS#12 files on the associated UC Application computer systems:

- 1) Copy the PKCS#12 file for the application computer under the name `tomcat-keystore.p12` to the following application computer directory:
`<SymphoniaHome>/common/conf`
- 2) If you use an active and a passive application computer: Execute step 1 on the second application computer also.
- 3) If you use Large Deployment: Copy the PKCS#12 file for the front-end computer under the name `tomcat-keystore.p12` to the following directory of a front-end computer.

`<SymphoniaHome>/common/conf`

- 4) If you use a Facade server: Copy the PKCS#12 file for the computer system of the Facade server under the name `OSC-Facade-Server-Default-Cert.p12` to the following directory of the relevant computer system:
- `/usr/local/tomcat6/conf`

10.15 Activating a Server Keystore for the CMP

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

How to configure the CMP for using individual certificates describes the *OpenScape Common Management Platform, Administrator Documentation* manual.

10.16 Configuring a Server Keystore for the Application Computer

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

The application computer communicates with different external systems – e. g. with OpenScape clients, a groupware server or an LDAP directory server. The application computer must use its certificate for this communication. This ensures the following:

- Application computers and external systems can authenticate themselves as permissible communication partners.
- Data can be transmitted encrypted.

So that an application computer uses its new certificate, the new keystore must be configured for the application computer.

Start the configuration

How to configure the new keystore for the application computer:

- 1) Open a shell on the application computer and log on as root user.
- 2) Check whether the following files are available on the application computer. If they are available, back them up.
 - `<CaDistribution>/ .keystore`
 - `<CaConfigHttpd>/Portal/ssl.cfg`
 - `<CaConfigHttpd>/CAMgmt/ssl.cfg`
- 3) Execute the following command to delete the previous keystore.

IMPORTANT: Verify that you have backed up the previous keystore in the precedent step.

```
rm -f <CaDistribution>/ .keystore
```

- 4) Execute the following command in one line to copy the new keystore.

```
cp "<SymphoniaHome>/common/conf/tomcat-keystore.p12"
"<CaDistribution>/ .keystore"
```

Configuring a Certificate Strategy

Configuring Certificate and Keys for the BCom Component

- 5) Execute the following command to transfer the new keystore to the OpenScape user **sym:sym**.

```
chown sym:sym "<CaDistribution>/ .keystore"
```

- 6) Start a text editor and open the following file therein:

```
<CaConfigHttpd>/Portal/ssl.cfg
```

- 7) Adjust the following entries in this file as described.

```
com.siemens.ca.server.SSLport.keystoreFile=.keystore
com.siemens.ca.server.SSLport.keystoreType=PKCS12
com.siemens.ca.server.SSLport.keystorePass=<Key/StorePassword>
```

- 8) Save the changes in the file.

- 9) Proceed as follows to reboot the web server components:

- a) Execute the following commands in order to restart the ucowcbe pod:

```
kubectl exec -it <ucowcbe_pod_name> -- bash kill 1
```

The relevant pod is being killed and restarted resulting in all settings performed so far to become effective.

- b) Execute the following commands in order to restart the uclwfe pod:

```
kubectl exec -it <uclwfe_pod_name> -- bash kill 1
```

The relevant pod is being killed and restarted resulting in all settings performed so far to become effective.

10.17 Configuring Certificate and Keys for the BCom Component

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

The BCom component of the application computer communicates for the client OpenScape Mobile by means of SOAP with OpenScape Voice systems connected to OpenScape UC Application using CSTA. To encrypt this communication and to authenticate against OpenScape Voice, the BCom component requires a pair of keys with associated certificate.

IMPORTANT: The certificate used must have been signed by the same certificate authority as the OpenScape Voice certificate. The BCom component can otherwise not communicate with OpenScape Voice.

Start the configuration

Execute the following steps to add the certificate and the pair of keys for the BCom component:

- 1) Execute the following command on the application server (BE pod):

```
cd <SymphoniaHome>/common/conf
```

- 2) Concatenate the application server's certificate and pair of keys in a temporary file by executing the following command:

```
cat tomcat_cert.pem keystore.pem > temp_cert.pem
```

tomcat_cert.pem contains the certificate and keystore.pem the pair of keys of the application computer.

NOTICE: You have created tomcat_cert.pem in Signing Certificate Sign Requests on page 716. You have created keystore.pem in Importing a Certificate in the Server Keystore on page 717.

- 3) Execute the following command in one line to add the certificate and pair of keys of the temporary file for the BCom component.



WARNING: The following command deletes the temporary file after certificate and pair of keys have been added for the BCom component.

```
/opt/siemens/servicetools/bcom/bcomImportCert.sh  
temp_cert.pem
```

NOTICE: The bcomImportCert.sh script can only process files in the PEM format.

- 4) Restart the UC Application services by restarting the BE pod using the following commands:

```
kubectl exec -it <ucbe_pod_name> -- bash kill 1
```

- 5) If you have enabled BE pod redundancy: Restart both BE pods.

10.18 Configuring a Server Keystore for the Multi-Node System

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

NOTICE: You need to execute the following additional steps for Large Deployment only.

For Large Deployment the various OpenScape components are distributed among different computer systems (application computer, frontend computer). The OpenScape components distributed in this way communicate with each other via TLS / SSL. This ensures the following:

- The various OpenScape components of the different computer systems can authenticate themselves as permissible communication partners
- Data can be transmitted encrypted.

The following specialties apply for the Large Deployment keystores:

- All frontend computers use the same key / the same certificate

- The keystores of the frontend computers are administered on the application computer.

Start the configuration

Configure TLS / SSL for Large Deployment by executing the following steps.

- 1) Open a shell on the application computer and log on as root user.
- 2) Check whether the following files are available on the application computer. If they are available, back them up.

- `<CaDistribution>/ .keystore`
- `<CaDistribution>/ .keystore`
- `<CaConfigHttpd>/Portal/ssl.cfg`
- `<CaConfigHttpd>/CAMgmt/ssl.cfg`

- 3) Execute the following command in one line to copy the keystore of the frontend computer to the application computer:

```
scp root@<FQHN of the front-end computer>:  
<SymphoniaHome>/common/conf/tomcat-keystore.p12  
<CaDistribution>/ .keystore
```

NOTICE: If the frontend computer cannot be authenticated, you need to confirm the connection to the frontend computer once again with **yes**.

- 4) Enter the root password for the frontend computer when you are prompted to.
- 5) Execute the following command to delete the previous camgmt-keystore of the application computer.

IMPORTANT: Verify that you have backed up the previous keystore in the precedent step.

```
rm -f <CaDistribution>/ .keystore
```

- 6) Execute the following command in one line to copy the new keystore of the application computer.

```
cp "<SymphoniaHome>/common/conf/tomcat-keystore.p12"  
"<CaDistribution>/ .keystore"
```

- 7) Execute the following command to transfer the new keystore to the OpenScape user **sym:sym**.

```
chown sym:sym "<CaDistribution>/ .keystore"  
"<CaDistribution>/ .keystore"
```

- 8) Start a text editor and open the following file therein:

```
<CaConfigHttpd>/Portal/ssl.cfg
```

- 9) Adjust the following entries in this file as described.

```
com.siemens.ca.server.SSLport.keystoreFile=.keystore  
com.siemens.ca.server.SSLport.keystoreType=PKCS12  
com.siemens.ca.server.SSLport.keystorePass=<Key/  
StorePassword for frontend keystore>
```

- 10) Save the changes in the file.

- 11) Start a text editor and open the following file therein:

`<CaConfigHttpd>/CAMgmt/ssl.cfg`

- 12) Adjust the following entries in this file as described.

```
com.siemens.ca.server.SSLport.keystoreFile=.keystore
com.siemens.ca.server.SSLport.keystoreType=PKCS12
com.siemens.ca.server.SSLport.keystorePass=<Key/
StorePassword for application computer>
```

- 13) Save the changes in the file.

- 14) Execute the following command to reboot the web server component of OpenScape UC Application on the application computer for the new settings to take effect.

`/etc/init.d/symphoniad restart WebClient_BE`

- 15) If you use an active and a passive application computer: Execute steps 1 to 14 for the second application computer also. Open a shell on the frontend computer and log on as root user. Execute the following command to reboot the web server component of OpenScape UC Application on the frontend computer for the new settings to take effect.

`/etc/init.d/symphoniad restart WebClient_FE`

- 16) If you use several frontend computers, execute steps 16 and 17 for each frontend computer.

10.19 Configuring a Server Keystore for the Facade Server

Execute these steps for:

CE 1	CE 2	CE 3	CE 4

NOTICE: You need to execute the following steps only if you use the OpenScape Mobile Client.

The Facade server communicates with the UC Application application computer within the company's own network and with the OpenScape Mobile Clients via internet. If SSL is configured for the Facade server, a standard certificate installed during the Facade server setup is used for this purpose. This ensures the following:

- The Facade server can identify itself as authorized communication partner against application computer and OpenScape Mobile Client
- Data can be transmitted encrypted.

So that the Facade server uses the new certificate, the new keystore must be configured for the Facade server.

Start the configuration

How to configure the new keystore for the Facade server:

- 1) Start a text editor on the computer system of the Facade server and open the following file therein:

`/usr/local/tomcat6/conf/server.xml`

Configuring a Certificate Strategy

Importing the Root Certificate in the Client Browsers

- 2) Search the file for the connector that communicates via SSL.

Example:

```
<Connector
    port="8443"
    SSLEnabled="true"
    acceptCount="20000"
    maxThreads="5000"
    scheme="https"
    secure="true"
    clientAuth="false"
    sslProtocol="TLS"
    keystoreFile="/usr/local/tomcat6/conf/OSC-Facade-
Server-Default-Cert.p12"
    ciphers="SSL_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_
RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_
EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA"
    keystoreType="PKCS12" keystorePass="<your_password>"
/>
```

- 3) Specify under the keystorePass parameter the new password you used while creating the keystore file for the Facade server.

Example:

```
<Connector
    port="8443"
    SSLEnabled="true"
    acceptCount="20000"
    maxThreads="5000"
    scheme="https"
    secure="true"
    clientAuth="false"
    sslProtocol="TLS"
    keystoreFile="/usr/local/tomcat6/conf/OSC-Facade-
Server-Default-Cert.p12"
    ciphers="SSL_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_
RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_
EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA"
    keystoreType="PKCS12" keystorePass="<your key / keystore
password>"
/>
```

- 4) Save the changes in the file.
- 5) Execute the following two commands to reboot the Facade server and for the performed changes to take effect.

```
/etc/init.d/catalinad stop
/etc/init.d/catalinad start
```

10.20 Importing the Root Certificate in the Client Browsers

Execute these steps for:



The UC Application computer systems authenticate themselves with their configured server certificates against the client browsers of the OpenScape users. So that the client browsers accept these server certificates you need to import the root certificate with which the server certificates of the OpenScape computer systems were signed in the client browsers of the UC Application users.

How this is done describes the product documentation for the client browsers used.

This chapter exemplifies the import of the root certificate in the Internet Explorer 8. The following steps are required:

- [Displaying the Root Certificate](#)
- [Checking the Root Certificate](#)
- [Installing the Root Certificate](#)

10.20.1 Displaying the Root Certificate

Execute these steps for:



Before you can import the root certificate in the Internet Explorer, you need to display it via the Internet Explorer.

Start the configuration

How to display the root certificate in the Internet Explorer 8:

- 1) Connect OpenScape UC Application via the Internet Explorer and HTTPS – e. g. using the OpenScape Web Client.

The Internet Explorer issues the following message to point out that it has received a seemingly invalid server certificate for the communication:

There is a problem with this website's security certificate.

- 2) Select the option **Continue to this website (not recommended)**.
- 3) The Internet Explorer shows the invoked internet page and points to the

certificate problem with  **Certificate Error** in the address bar.

- 4) Click on **Certificate Error**.

A message window opens.

- 5) In the message window click on **View Certificates**.

A dialog that displays all information of the server certificate opens.

- 6) Switch to the **Certification Path** tab.

- 7) Select the root certificate that is marked as invalid (.

- 8) Click on **View Certificate**.

A dialog that displays all information of the root certificate opens.

10.20.2 Checking the Root Certificate

Execute these steps for:



Before you import the displayed root certificate in the Internet Explorer, check it. This will reveal whether the root certificate is actually the original one used.

Start the configuration

How to check the displayed root certificate in the Internet Explorer 8:

- 1) In the dialog that contains the root certificate information switch to the **Details** tab.
- 2) Select the **Thumbprint** field.
- 3) Compare the displayed thumbprint with the one of the original root certificate used.

IMPORTANT: Both thumbprints must match.

If both thumbprints match, the received server certificate was actually signed with the original root certificate. The received server certificate can then be considered trustworthy.

10.20.3 Installing the Root Certificate

Execute these steps for:



After checking the displayed root certificate has proved it to be trustworthy, you can import it in the Internet Explorer.

Start the configuration

How to import the root certificate in the Internet Explorer 8:

- 1) In the dialog that contains the root certificate information switch to the **General** tab.
- 2) Click on **Install Certificate...**
The Certificate Import Wizard opens.
- 3) Click on **Next**.
- 4) Select the option **Automatically select the certificate store based on the type of certificate**.
- 5) Click on **Next**.
- 6) Check the displayed import settings. When all settings are correct, click on **Finish**.
A security warning is displayed. It shows the thumbprint of the certificate to be imported.
- 7) Check once again whether the displayed thumbprint matches the one of the original root certificate.
- 8) If the thumbprints match, confirm the security warning with **Yes**.

A message informs you that the root certificate has been successfully imported in the Internet Explorer.

10.21 Importing the Root Certificate in the Mobile Phones

Execute these steps for:



NOTICE: You need to execute the following steps only if you use the OpenScape Mobile Client.

The Facade server with its configured server certificate identifies itself against the mobile phones used. So that the mobile phones accept this server certificate, you need to import the root certificate with which the Facade server certificate was signed in the mobile phones of the OpenScape users.

The root certificate can be generally provided for OpenScape users via the download page of the Facade server. If you cannot access this download page, you need to import the root certificate in the mobile phones in another way. How to proceed is described in the product documentation for the mobile phones used.

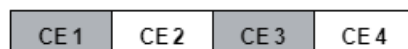
Start the configuration

Provide OpenScape users with the root certificate via the download page of the Facade server by overriding the following file with the cer file of the root certificate on the Facade server's computer system:

```
/usr/local/facade/apache-tomcat-<version>/webapps/  
download/OBSO.cer
```

10.22 Configuring the Certificate for the SPML Interface

Execute these steps for:



NOTICE: You need to execute the following steps only if you use the SPML¹⁰⁰ interface of OpenScape UC Application. This is the case when you use customer-specific applications connected to OpenScape UC Application via the SPML interface. Examples of such applications are the components HPUM and OSILA. You find detailed information about using the SPML interface in the OpenScape UC Application SPML SDK, Programming Guide.

If a user accesses the SPML interface of the application computer with the help of an SPML-based client, the client can check whether the server certificate of

¹⁰⁰ The SPML interface provides an SOAP-based access to the OpenScape UC Application features.

the SPML responder is valid. This will ensure that data is transmitted encrypted between SPML client and SPML responder.

The keystore of the SPML responder contains already a pre-installed self-signed default certificate inclusive private key. If required, you can replace both of them, thus adjusting them to an individual certificate strategy.

To replace the pre-installed default certificate and the associated private key, you need a password-protected PKS#12 keystore file that contains the certificate to be newly used and the associated private key. This keystore file can be provided by an official certificate authority; but you can also create it by yourself as described in this manual for other components.

IMPORTANT: If not only the keystore file is password-protected but the key contained therein too, key and keystore password must be identical.

Start the configuration

Replace the default certificate and private key for the SPML responder by executing the following steps:

- 1) Open a shell on the relevant computer system and log on as root user.
- 2) Copy the provided PKS#12 keystore file under the name `spmlresponder_keystore.p12` to the following application computer directory:

```
<SymphoniaHome>/common/conf
```

- 3) Execute the following commands to assign the keystore file to the SPML responder and to set the required access privileges.

```
chown sym spmlresponder-keystore.p12
chgrp sym spmlresponder-keystore.p12
chmod 644 spmlresponder-keystore.p12
```

- 4) Start a text editor and open the following file therein:

```
<SymphoniaHome>/common/conf
```

- 5) Find in the file the connector for which the following has been configured:

```
name="spmlresponder_https_connector"
port="9943"scheme="https"
```

- 6) Adjust the settings of the relevant connector as follows:

```
<Connector
...
    cmpPassphraseProtect="true"
    keystoreType="PKCS12"
    keystoreFile="< SymphoniaHome >/share/tomcat/conf/
spmlresponder_keystore.p12"
    keystorePass=" < your key / keystore password > "
...
/>
```

To encrypt the password, use the following script: `encodePassphrase.sh`

- 7) Save the changes in the `server.xml` file.

- 8) Execute the following command to reboot the Tomcat web server of OpenScape UC Application for the new settings to take effect.

```
/etc/init.d/symphoniad restart TomcatServletContainer
```

10.23 Configuring the Certificate for the UC Graph Connector

The Graph connector can also be configured to use a custom certificate instead of the included default one. To make this change, a keystore has to be created (can be either JKS or PKCS12) and should host a valid customer certificate issued for the facade node. The certificate must be accompanied with its private RSA key within the keystore that will be used by the UC graph connector.

This keystore can be used by the graph connector after modifying `/opt/uc-graph-connector/application.properties` to include the `server.ssl.key-store` (the location of the keystore in filesystem), `server.ssl.key-store-password` (the password of the keystore), `server.ssl.keyStoreType` (the type of keystore properties. JKS or PKCS12) and `server.ssl.keyAlias` (the alias of the certificate inside the keystore) properties.

To explicitly define the supported ciphers, you need to add the `server.ssl.ciphers` property and provide the required comma separated cipher list.

To apply the changes, you must restart the graph connector.

For example:

```
server.ssl.key-store = file:/opt/graph/JKSkeystore.jks
```

```
server.ssl.key-store-password = P@ssword
```

```
server.ssl.keyStoreType = JKS
```

```
server.ssl.keyAlias = graphconnector
```

```
server.ssl.ciphers =
```

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_1
```

10.24 Supplementing Instructions

You may need the following additional instructions to configure the certificate strategy in a customer environment.

- [Creating a secure Password](#)
- [Combining Certificate Files to a Certificate Chain](#)
- [Converting the Format of a Certificate Chain from DER into PEM](#)
- [Converting the Format of a Certificate Chain from PKCS#12 into PEM](#)

10.24.1 Creating a secure Password

Certificates and keys are stored in the so-called keystore of a computer system. Creating such a keystore for accessing it later requires a keystore password. To protect the keystore from unauthorized access effectively, this password should comprise a character string generated arbitrarily.

Each pair of keys of a keystore can also be protected from unauthorized access by a key password. This key password, however, must usually correspond to the keystore password.

Start the configuration

How to create a random password by executing the following steps on an UC Application computer system:

- 1) Open a shell.
- 2) Execute the following command in one line:

```
dd if=/dev/urandom bs=128 count=1 2>/dev/null |  
od -t o1 -w1 | awk '{v=$2%200;  
if(v>=40 && v<177 && !match(v,"",/^(4[0267]|7[46]|  
177)$/))  
system("echo -ne \\\\\\\\"v)}' |  
awk '{print substr($0,2,8)}'
```

You see an randomly created password, which may contain the following characters:

- Letters A to Z and a to z
- Digits 0 to 9
- The special characters !\$() * + , - . / : ; = ? @ [\] ^ _ ` { | } ~

The following characters are excluded since they may cause problems when being processed at a later date.

- Blank
- "&'<>

The created password comprises eight characters. If you want to create a longer password, specify the desired number of characters in the bolded term of the command as follows:

```
print substr($0,2,<number of characters>)
```

IMPORTANT: The password should comprise at least eight characters for security reasons.

- 3) Keep the created password in mind.

10.24.2 Combining Certificate Files to a Certificate Chain

Several certificates may have to be combined to a certificate chain. This is especially the case when, besides a root certificate, further intermediate certificates are required to prove a certificate trustworthy.

Start the configuration

How to combine several certificates to a certificate chain by executing the following steps on an UC Application computer system:

- 1) Open a shell and log on as root user.
- 2) Execute the following command:

```
cd <SymphoniaHome>/common/conf
```

- 3) Execute the following command in one line to combine a root certificate `ca_root.pem` with the intermediate certificates `im_cert1.pem` and `im_cert2.pem`.

NOTICE: You can shorten or extend the certificate list at will.

```
cat ca_root.pem
im_cert1.pem
im_cert2.pem >
ca_chain.pem
```

The newly created certificate chain is stored under the name `ca_chain.pem` in the current directory.

10.24.3 Converting the Format of a Certificate Chain from DER into PEM

You can convert a certificate chain into the PEM format if it is available in the DER format.

Start the configuration

How to convert a certificate chain from the DER format into the PEM format by executing the following steps on an UC Application computer system:

- 1) Open a shell and log on as root user.
- 2) Execute the following command:
`cd <SymphoniaHome>/common/conf`
- 3) Execute the following command in one line to convert the certificate chain `ca_chain.der` into the PEM format.

```
openssl x509
-in ca_chain.der
-inform DER
-out ca_chain.pem
-outform PEM
```

The converted certificate chain is stored under the name `ca_chain.pem` in the current directory.

10.24.4 Converting the Format of a Certificate Chain from PKCS#12 into PEM

You can convert a certificate chain into the PEM format if it is available in the PKCS#12 format.

Start the configuration

How to convert a certificate chain from the PKCS#12 format into the PEM format by executing the following steps on an UC Application computer system:

- 1) Open a shell and log on as root user.

Configuring a Certificate Strategy

- 2) Execute the following command:

```
cd <SymphoniaHome>/common/conf
```

- 3) Execute the following command to convert the certificate chain `ca_chain.pfx` into the PEM format.

```
openssl pkcs12 -in ca_chain.pfx -out ca_chain.pem
```

The converted certificate chain is stored under the name `ca_chain.pem` in the current directory.

11 IPsec Configuration

This chapter provides information about the following topics:

- [Using IPsec](#)
- [Configuring IPsec for CSTA Connections](#)
- [Configuring IPsec for MGCP Connections](#)
- [Operating System Upgrade SLES 12 SP4/SP5](#)

NOTICE: All information about Large Deployment apply likewise for Very Large Deployment.

11.1 Using IPsec

During operation, OpenScape UC Application and OpenScape Voice exchange sensitive data using the MGCP and CSTA protocols. Always make sure to protect such data from unauthorized access.

The most simple way to achieve this is operating all involved systems in a common, protected sub-network. This is in particular possible for Integrated Deployment.

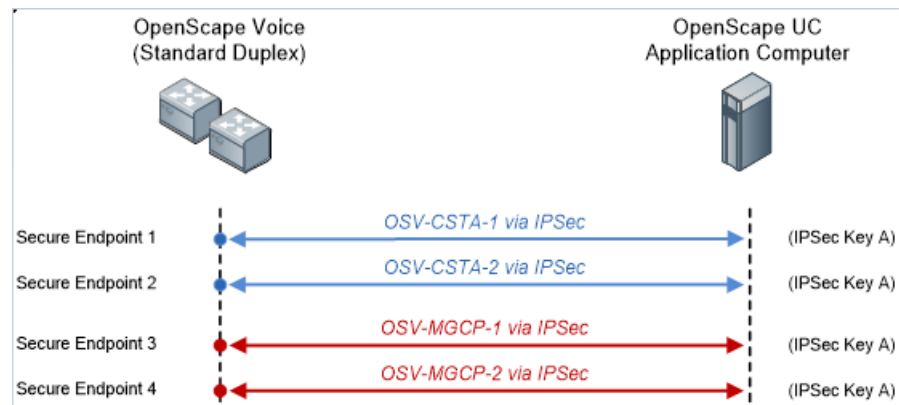
If you operate the various system components in different or even unprotected sub-networks, communication between these components must be encrypted. For this job we recommend IPsec, which establishes connection tunnels between the systems involved. Data transmitted through such a connection tunnel is encrypted by IPsec and consequently protected from unauthorized access.

To use IPsec tunnels in OpenScape Voice, a so-called secure end point is configured there for each tunnel. A target system and an IPsec key is assigned to such an end point.

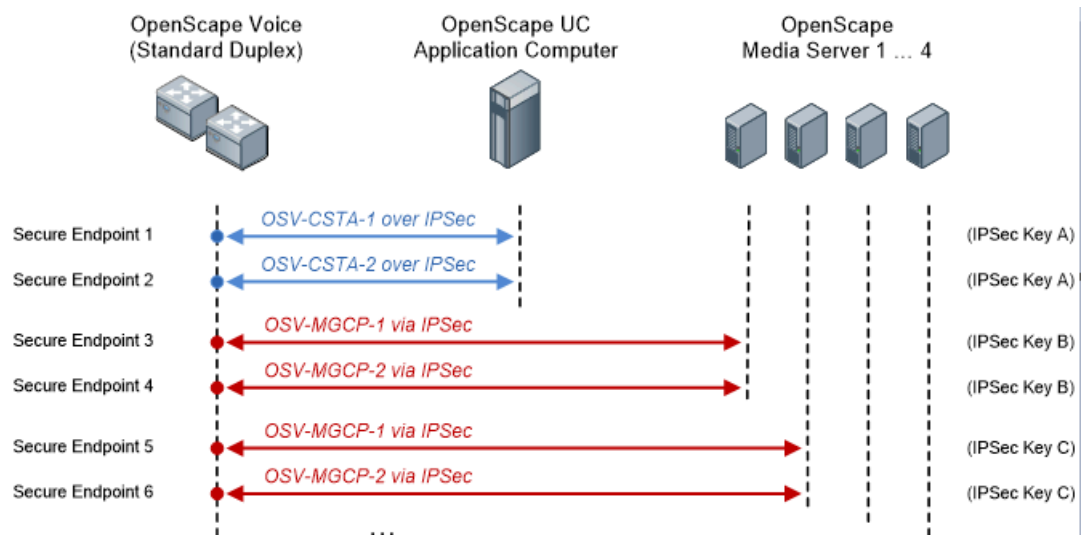
NOTICE: If OpenScape Voice is to use several IPsec tunnels to a common target system, the same key must be configured in OpenScape Voice for the associated secure end points.

The computer systems of OpenScape UC Application are configured for IPsec with the help of a configuration file.

Using IPsec for OpenScape UC Application – Small Deployment



Using IPsec for OpenScape UC Application – Large Deployment



11.2 Configuring IPsec for CSTA Connections

You need to execute the following configuration steps for encrypting the CSTA connections between OpenScape UC Application and OpenScape Voice using IPsec.

- [Configuring OpenScape Voice for IPsec-based CSTA Connections](#)
- [Configuring OpenScape UC Application for IPsec-based CSTA Connections](#)

11.2.1 Configuring OpenScape Voice for IPsec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape UC Application by IPsec requires configuring IPsec in OpenScape Voice.

NOTICE: You need to execute the configuration steps for OpenScape Voice (Standard Duplex) on one of the two system

nodes only. All settings are automatically transmitted from the configured system node to the second system node.

Start the configuration

How to configure IPsec for OpenScape Voice:

- 1) Start the RTP Command Line Interface (startCli) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
- 2) Select:
 - Main Menu > Application-level Management >**
 - Network Element Security Management >**
 - Secure End Point Device Security Management**
- 3) Create a secure end point for the IP address of the first CSTA interface of OpenScape Voice.

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)>
  (default: ): <Unique Name for the CSTA Endpoint>
Description <Max Length 63 (max length: 63)>
  (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP
  Addr. of the UC Application Computer>
Remote NetMask < (max length: 15)> (default: ):
Remote Port <0 = All Ports>:
Local Host < (max length: 32)>
  (default: ): <csta_ip_alias_1>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
  (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)>
  (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input>
  (default: 1): 1
Key Type <1 = ascii 1,2 = hex> (default: 1): 2
Key Length in Bytes (default: 16):
Do you want to execute this action? <y/n> (default:
yes):
```

Operation successful

NOTICE: If you do not specify an IP address but the associated fully qualified host name under Local Host, you need not modify the IPsec configuration in the event that the IP address of the relevant interface changes at a later date. The fully qualified host names for CSTA are defined for OpenScape Voice in /etc/hosts. They read by default **csta_ip_alias_1** and **csta_ip_alias_2**.

- 4) Determine the key used for the tunnel of the first CSTA interface. To do so, display the settings of the just created end point as shown in the following example.

Example:

```
Selection (default: 3): 4
Secure End Point Name <Max Length 63 (max length: 63)>
  (default: ): <name of the created CSTA end point>
Do you want to execute this action? <y/n> (default:
  yes): y
Total Number of SecEndPts Retrieved : 1
Name: Ext_Asst
Description:
FQDN:
Remote IP Address: <Ext_Asst_IP_Address>
Remote NetMask:
Remote Port : 0
Local Host: bond_node_alias
Local Port: 0
IPsec Profile: IPSEC_ESP_SHA_AES
IKE Profile: IKE_SHA2_AES
Key Gen Method: Automatic
Key Type: Hex
Key Length: 16

Key: 7aa88aec7f40699884b75795fbf9354
```

- 5) Note down the **Key**: output.
- 6) Create a secure end point for the second CSTA interface of OpenScape Voice. Because the relevant IPsec tunnel will later lead to the same application computer as for the first end point, you need to use the same key – the one you just noted down. Proceed as shown in the following example:

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)>
  (default: ): <Unique Name for the CSTA Endpoint>
Description <Max Length 63 (max length: 63)>
  (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address <(max length: 15)> (default: ): <IP
  Addr. of the UC Application Computer>
Remote NetMask <(max length: 15)> (default: ):
Remote Port <0 = All Ports>:
Local Host <(max length: 32)>
  (default: ): <csta_ip_alias_2>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
  (default: ): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)>
  (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input>
  (default: 1): 2
```

```
Key Length in Bytes (default: 16): <Key of the first
CSTA Endpoint>
```

```
Do you want to execute this action? <y/n> (default:
yes):
```

```
Operation successful
```

You have now configured IPsec for the CSTA connection in OpenScape Voice.

11.2.2 Configuring OpenScape UC Application for IPsec-based CSTA Connections

Encrypting the CSTA communication between OpenScape Voice and OpenScape UC Application by IPsec requires configuring IPsec on the application computer of OpenScape UC Application.

The RPM `strongSwan` must be installed and configured on the relevant computer system for this purpose. This RPM is already contained in the SLES repository of every UC Application system.

NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
 - SLES 15 SP5, for UC V11R6
-

Start the configuration

How to configure IPsec for the application computer:

- 1) Place the SLES DVD in the application computer drive.
- 2) If you have not integrated the SLES DVD as additional installation source yet, do it now via the `zypper ar` command.
- 3) Execute the following command to install the RPM `strongSwan`:
`zypper in strongSwan`
- 4) Open the following configuration file in a text editor:
`/etc/ipsec.conf`
- 5) In the `Add connections` here section, define an IPsec connection for each CSTA end point you have configured in OpenScape Voice.

In doing so, use the following format:

```
conn %default

    rekeymargin=3m
    keyingtries=1
    mobike=no

# Add connections here.
conn <unique connection name>
```

```
keyexchange=ikev2
left=<IP addr. of the CSTA interface of
OpenScape Voice>
right=<IP addr. of the UC application computer>
leftprotoport=%any/%any
rightprotoport=%any/%any
leftfirewall=no
auto=start
authby=secret
keylife=1440s
ikelifetime=3600s
dpddelay=30
dpdtimeout=150
dpdaction=hold
type=transport
ike=aes128-sha256-modp2048
esp=aes128-sha256-modp2048
```

- 6) Save the changes in the configuration file.
- 7) Open the following configuration file in a text editor:
/etc/ipsec.secrets
- 8) At the end of the configuration file, define the key to be used for encrypting the CSTA data. This is the key you noted down during the IPsec configuration of OpenScape Voice.

In doing so, use the following format:

```
<IP addr. of the UC Application computer>
<IP addr. of the CSTA interface of OpenScape Voice> :
PSK 0x<key>
```

Example:

```
10.235.85.20 10.235.98.58 : PSK
0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.20 10.235.98.59 : PSK
0xc3daff51c40778fe2a92f31ecb93e653
```

NOTICE: Both CSTA interfaces of OpenScape Voice (10.235.98.58 / 59) end on the same application computer (10.235.85.20). This is why the connections use the same key.

IMPORTANT: There must be a space between the IP-Address and the colon (":")

NOTICE: Leave the configuration file otherwise unchanged.

- 9) Save the changes in the configuration file.
- 10) Open file /etc/strongswan.conf

11) Modify the file to include the following:

```
# strongswan.conf - strongSwan configuration file
charon
{
    # number of worker threads in charon      threads =
    16
    # plugins to load in charon
    # load = aes des sha1 md5 sha2 hmac gmp random
    pubkey xcbc x509 stroke
    plugins {
        sql
        {
            # loglevel to log into sql database
            loglevel = -1
            # URI to the database
            # database = sqlite:///path/to/file.db
            # database = mysql://user:password@localhost/
database
        }
        duplicheck
        {
            # Enable duplicheck plugin (if loaded).
            # enable = yes
enable = no

            # Whether to load the plugin. Can also be an
integer to increase the
            # priority of this plugin.
load = no

            # Socket provided by the duplicheck plugin.
            # socket = unix${piddir}charon.dck
        }
    }
# filelog
# {
#     /log/ipsec.log
#     {
#         # add a timestamp prefix
#         time_format = %y%m%d-%H%M%S
#         # prepend connection name, simplifies grepping
#         ike_name = yes
#         # overwrite existing files
#         append = yes
#         # increase default loglevel for all daemon
# subsystems
#         default = 1
#         # flush each line to disk
#         flush_line = yes
#     }
# }
stderr
{
    # more detailed loglevel for a specific
subsystem, overriding the
```

```
# default loglevel.
ike = -1
kn1 = -1
enc = -1
net = -1
} # ...
syslog {
    # prefix for each log message
    identifier = charon
    # use default settings to log to the LOG_DAEMON
    facility
    daemon {
        default = -1
        ike = -1
        enc = -1
        net = -1
    }
    # very minimalistic IKE auditing logs to
    LOG_AUTHPRIV
    auth {
        default = -1
        ike = -1
    }
}
}
pluto
{
    # plugins to load in pluto
    # load = aes des sha1 md5 sha2 hmac gmp random
    pubkey } libstrongswan
{
    # set to no, the DH exponent size is optimized
    # dh_exponent_ansi_x9_42 = no
}
```

- 12)** To start the IPsec service, execute the following command as root in a shell:

```
ipsec start
```

NOTICE: Every time you modify the IPSEC rules a new `ipsec restart` is necessary. With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

- 13)** To have the IPsec service started automatically when the application computer reboots, execute the following command as root in a shell:

```
chkconfig ipsec on
```

NOTICE: In SLES 12 installations IPsec can be enabled and started via the following commands:

```
systemctl enable strongswan.service
systemctl start strongswan.service
systemctl status strongswan.service
```

- 14) To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump -i any | grep ESP
```

If OpenScape Voice and OpenScape UC Application communicate via CSTA, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsalln1:  
  ESP(spi=0xfb1c7d52,seq=0x16)  
17:09:23.064081 IP adsalln1 > 10.1.250.20:  
  ESP(spi=0x39281790,seq=0x16)  
17:09:23.064086 IP adsalln1 > 10.1.250.20:  
  ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for CSTA connections between OpenScape Voice and OpenScape UC Application.

11.3 Configuring IPsec for MGCP Connections

NOTICE: You need to execute the configuration steps of this chapter only if you use the OpenScape Media Server of OpenScape UC Application also as Media Server Stand-alone) for OpenScape Voice.

The steps you execute to configure IPsec for MGCP connections depend on whether you use OpenScape UC Application as Small Deployment or Large Deployment.

- [Configuration for Small Deployment](#)
- [Configuration for Large Deployment](#)

11.3.1 Configuration for Small Deployment

NOTICE: You need to execute the configuration steps of this chapter only if you use Small Deployment.

You must execute the following configuration steps for encrypting the MGCP connections between OpenScape UC Application (Small Deployment) and OpenScape Voice using IPsec.

- [Configuring OpenScape Voice for IPsec-based MGCP Connections \(Small Deployment\)](#)
- [Configuring OpenScape UC Application for IPsec-based MGCP Connections \(Small Deployment\)](#)

11.3.1.1 Configuring OpenScape Voice for IPsec-based MGCP Connections (Small Deployment)

Encrypting the MGCP communication between OpenScape Voice and the OpenScape Media Server by IPsec requires configuring IPsec in OpenScape Voice.

Start the configuration

Configure IPsec for OpenScape Voice by executing the following steps:

- 1) Start the RTP Command Line Interface (startCli) on one of the OpenScape Voice (Standard Duplex) nodes and log in there as **sysad**.
- 2) Select:
 - Main Menu > Application-level Management >**
 - Network Element Security Management >**
 - Secure End Point Device Security Management**
- 3) Create a secure end point for the fully qualified host name of the first MGCP interface of OpenScape Voice.

Because the relevant IPsec tunnel will later be set up to the application computer of OpenScape UC Application also, you must use the same key as for the CSTA tunnels. Proceed as shown in the following example:

Example:

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)>
  (default: ): <Unique Name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)>
  (default: ):
FQDN <Max Length 63 (max length: 63)> (default: ):
Remote IP Address < (max length: 15)> (default: ): <IP
  Addr. of the UC Application Computer>
Remote NetMask < (max length: 15)> (default: ):
Remote Port <0 = All Ports>:
Local Host < (max length: 32)>
  (default: ): ncs_ip_alias_1
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
  (default: ): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)>
  (default: ): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input>
  (default: 1): 2
Key Length in Bytes (default: 16): <Key of the CSTA
  Endpoints>
Do you want to execute this action? <y/n> (default:
yes):
```

Operation successful

NOTICE: If you do not specify an IP address but the associated fully qualified host name under Local Host, you need not modify the IPsec configuration in the event

that the IP address of the relevant interface changes at a later date. The fully qualified host names for MGCP are defined for OpenScape Voice in `/etc/hosts`. They read `ncs_ip_alias_1` and `ncs_ip_alias_2` by default.

- 4) Create a secure end point for the second MGCP interface of OpenScape Voice in the same way. But use the expression `ncs_ip_alias_2` instead of `ncs_ip_alias_1` under Local Host.

You have now configured IPsec for the MGCP connection in OpenScape Voice.

11.3.1.2 Configuring OpenScape UC Application for IPsec-based MGCP Connections (Small Deployment)

Encrypting the MGCP communication between OpenScape Voice and OpenScape Media Server by IPsec requires configuring IPsec on the application computer of OpenScape UC Application.

The RPM `strongSwan` must be installed and configured on the relevant computer system for this purpose. This RPM is already contained in the SLES repository of every UC Application system.

NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
 - SLES 15 SP5, for UC V11R6
-

Start the configuration

Configure IPsec for the application computer by executing the following steps:

- 1) Place the SLES DVD in the application computer drive.
- 2) If you have not integrated the SLES DVD as additional installation source yet, do it now via the `zypper ar` command.
- 3) Execute the following command to install the RPM `strongSwan`:
`zypper in strongSwan`
- 4) Open the following configuration file in a text editor:
`/etc/ipsec.conf`
- 5) Remove the following sections from the configuration file:
 - default settings for connections
 - sample VPN connection

IMPORTANT: Do not delete section `Disable Opportunistic Encryption`. The relevant computer system will otherwise lose its network connection as soon as IPsec starts.

- 6) In the Add connections here section, define an IPsec connection for each MGCP end point you have configured in OpenScape Voice.

In doing so, use the following format:

```
conn %default
    rekeymargin=3m
    keyingtries=1
    mobike=no

# Add connections here.
conn <unique connection name>

    keyexchange=ikev2
    left=<IP addr. of the MGCP interface of
OpenScape Voice>
    right=<IP addr. of the UC application computer>
leftprotoport=%any/%any
rightprotoport=%any/%any
leftfirewall=no
    auto=start
    authby=secret
    keylife=1440s
    ikelifetime=3600s
    dpddelay=30
    dpdtimeout=150
    dpdaction=hold
    type=transport
    ike=aes128-sha256-modp2048
    esp=aes128-sha256-modp2048
```

- 7) Save the changes in the configuration file.
- 8) Open the following configuration file in a text editor:
- ```
/etc/ipsec.secrets
```
- 9) At the end of the configuration file, define the key to be used for encrypting the MGCP data. This is the key you noted down during the IPsec configuration of OpenScape Voice.

In doing so, use the following format:

```
<IP addr. of the application computer>
<IP addr. of the MGCP interface of OpenScape Voice> :
 PSK 0x<key>
```

**Example:**

```
10.235.85.22 10.235.98.60 : PSK
 0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.22 10.235.98.61 : PSK
 0xc3daff51c40778fe2a92f31ecb93e653
```

---

**NOTICE:** In the example, both MGCP connections of OpenScape Voice (10.235.98.60 / 61) end on the

application computer (10.235.85.22). This is why the connections use the same key.

---

**IMPORTANT:** There must be a space between the IP-Address and the colon (":")

---



---

**NOTICE:** Leave the configuration file otherwise unchanged.

---

- 10) Save the changes in the configuration file.
- 11) Open file /etc/strongswan.conf
- 12) Modify the file in order to include the following

```
strongswan.conf - strongSwan configuration file
charon
{
 # number of worker threads in charon
 threads = 16
 # plugins to load in charon
 # load = aes des sha1 md5 sha2 hmac gmp random
 pubkey xcbc x509 stroke

 plugins {
 sql
 {
 # loglevel to log into sql database
 loglevel = -1
 # URI to the database
 # database = sqlite:///path/to/file.db
 # database = mysql://user:password@localhost/
 }
 }

 database
 {
 }

 duplicheck
 {
 # Enable duplicheck plugin (if loaded).
 # enable = yes
 enable = no
 # Whether to load the plugin. Can also be an
 integer to increase the
 # priority of this plugin.
 load = no
 # Socket provided by the duplicheck plugin.
 # socket = unix${piddir}charon.dck
 }
}

filelog
{
/log/ipsec.log
{
add a timestamp prefix
time_format = %y%m%d-%H%M%S
prepend connection name, simplifies grepping
ike_name = yes
}
}
```

```
overwrite existing files
append = yes
increase default loglevel for all daemon
#subsystems
default = 1
flush each line to disk
flush_line = yes
}
}
 stderr
 {
 # more detailed loglevel for a specific
 subsystem, overriding the
 # default loglevel.
 ike = -1
 kn1 = -1
 enc = -1
 net = -1
 }
 # ...
 syslog
 # prefix for each log message
 identifier = charon
 # use default settings to log to the LOG_DAEMON
 facility
 daemon {
 default = -1
 ike = -1
 enc = -1
 net = -1
 }
 # very minimalistic IKE auditing logs to
 LOG_AUTHPRIV
 auth {
 default = -1
 ike = -1
 }
}
pluto
{
 # plugins to load in pluto
 # load = aes des sha1 md5 sha2 hmac gmp random
 pubkey
}
libstrongswan
{
 # set to no, the DH exponent size is optimized
 # dh_exponent_ansi_x9_42 = no
}
```

- 13) To start the IPsec service, execute the following command as root in a shell:

```
ipsec start
```

---

**NOTICE:** Every time you modify the IPSEC rules a new `ipsec restart` is necessary. With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

---

- 14) To have the IPsec service start automatically when the application computer reboots, execute the following command as root in a shell:

```
chkconfig ipsec on
```

---

**NOTICE:** In SLES 12 installations IPsec can be enabled and started via the following commands: `systemctl enable strongswan.service` `systemctl start strongswan.service` `systemctl status strongswan.service`

---

- 15) To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump -i any | grep ESP
```

If OpenScape Voice and application computers communicate via MGCP, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsalln1:
 ESP(spi=0xfb1c7d52,seq=0x16)
17:09:23.064081 IP adsalln1 > 10.1.250.20:
 ESP(spi=0x39281790,seq=0x16)
17:09:23.064086 IP adsalln1 > 10.1.250.20:
 ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for MGCP connections between OpenScape Voice and OpenScape UC Application.

## 11.3.2 Configuration for Large Deployment

---

**NOTICE:** You need to execute the configuration steps of this chapter only if you use Large Deployment.

---

You must execute the following configuration steps for encrypting the MGCP connections between OpenScape UC Application (Large Deployment) and OpenScape Voice using IPsec.

- [Configuring OpenScape Voice for IPsec-based MGCP Connections \(Large Deployment\)](#)
- [Configuring OpenScape UC Application for IPsec-based MGCP Connections \(Large Deployment\)](#)

### 11.3.2.1 Configuring OpenScape Voice for IPsec-based MGCP Connections (Large Deployment)

Encrypting the MGCP communication between OpenScape Voice and the relevant OpenScape Media Servers by IPsec requires configuring IPsec in OpenScape Voice.

#### Start the configuration

Configure IPsec for OpenScape Voice by executing the following steps:

- 1) Create a secure end point for the fully qualified host name **ncs\_ip\_alias\_1**.

*Example:*

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)>
 (default:): <Unique Name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)>
 (default:):
FQDN <Max Length 63 (max length: 63)> (default:):
Remote IP Address < (max length: 15)> (default:): <IP
 Addr. of the Media Server MGCP Interface>
Remote NetMask < (max length: 15)> (default:):
Remote Port <0 = All Ports>:
Local Host < (max length: 32)>
 (default:): ncs_ip_alias_1
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
 (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)>
 (default:): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input>
 (default: 1): 1
Key Type <1 = ascii 1, 2 = hex> (default: 1): 2
Key Length in Bytes (default: 16):
Do you want to execute this action? <y/n> (default:
 yes):
```

Operation successful

---

**NOTICE:** If you do not specify an IP address but the associated fully qualified host name under Local Host, you need not modify the IPsec configuration in the event that the IP address of the relevant interface changes at a later date. The fully qualified host names for MGCP are defined for OpenScape Voice in /etc/hosts. They read **ncs\_ip\_alias\_1** and **ncs\_ip\_alias\_2** by default.

---

- 2) Determine the key the secure end point uses for the tunnel of the first MGCP interface by having the settings of the just created end point displayed. Proceed as shown in the following example:

*Example:*

```
Selection (default: 3): 4
```

```
Secure End Point Name <Max Length 63 (max length: 63)>
 (default:): <name of the created MGCP end point>
Do you want to execute this action? <y/n> (default:
 yes): y
Total Number of SecEndPts Retrieved : 1
Name: Ext_Asst
Description:
FQDN:
Remote IP Address: <Ext_Asst_IP_Address>
Remote NetMask:
Remote Port : 0
Local Host: bond_node_alias
Local Port: 0
IPsec Profile: IPSEC_ESP_SHA_AES
IKE Profile: IKE_SHA2_AES
Key Gen Method: Automatic
Key Type: Hex
Key Length: 16
```

Key: **7aa88aecdf40699884b75795fbf9354**

- 3) Note down the **Key**: output. Create a secure end point for the fully qualified host name of the second MGCP interface of OpenScape Voice. Because the relevant IPsec tunnel will later be set up to the same OpenScape Media Server as for the first end point, you need to use the same key – the one you just noted down. Proceed as shown in the following example:

*Example:*

```
Selection (default: 3): 1
Secure End Point Name <Max Length 63 (max length: 63)>
 (default:): <Unique Name for the MGCP Endpoint>
Description <Max Length 63 (max length: 63)>
 (default:):
FQDN <Max Length 63 (max length: 63)> (default:):
Remote IP Address <(max length: 15)> (default:): <IP
 Addr. of the Media Server MGCP Interface>
Remote NetMask <(max length: 15)> (default:):
Remote Port <0 = All Ports>:
Local Host <(max length: 32)>
 (default:): ncs_ip_alias_2
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
 (default:): IPSEC_ESP_SHA_AES
IKE Profile Name <Max Length 63 (max length: 63)>
 (default:): IKE_SHA2_AES
Key Generation Method <1 = automatic, 2 = user input>
 (default: 1): 2
Key Length in Bytes (default: 16): <Key of the first
 MGCP Endpoint>
Do you want to execute this action? <y/n> (default:
 yes):

Operation successful
```

- 4) If you use several OpenScape Media Servers as Media Server for OpenScape Voice, execute steps 1 to 4 for the MGCP interface of the relevant OpenScape Media Servers.

In doing so, use an individual key for each OpenScape Media Server.

You have now configured IPsec for the MGCP connection in OpenScape Voice.

### 11.3.2.2 Configuring OpenScape UC Application for IPsec-based MGCP Connections (Large Deployment)

Encrypting the MGCP communication between OpenScape Voice and the relevant OpenScape Media Servers by IPsec requires configuring IPsec on every involved OpenScape Media Server.

The RPM `strongSwan` must be installed and configured on the relevant computer system for this purpose. This RPM is already contained in the SLES repository of every UC Application system.

---

#### NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
  - SLES 15 SP5, for UC V11R6
- 

#### Start the configuration

How to configure IPsec for an involved OpenScape Media Server:

- 1) Place the SLES DVD in the application computer drive.
- 2) If you have not integrated the SLES DVD as additional installation source yet, do it now via the `zypper ar` command.
- 3) Execute the following command to install the RPM `strongSwan`:  

```
zypper in strongSwan
```
- 4) Open the following configuration file in a text editor:  
`/etc/ipsec.conf`
- 5) Remove the following sections from the configuration file:
  - `default settings for connections`
  - `sample VPN connection`

---

**IMPORTANT:** Do not delete section `Disable Opportunistic Encryption`. The relevant computer system will otherwise lose its network connection as soon as IPsec starts.

---

- 6) In the `Add connections here` section, define an IPsec connection for each MGCP end point you have configured in OpenScape Voice for the relevant OpenScape Media Server.

In doing so, use the following format:



```

conn %default
 rekeymargin=3m
 keyingtries=1
 mobike=no

Add connections here.
conn <unique connection name>

 keyexchange=ikev2
 left=<IP addr. of the MGCP interface of
OpenScape Voice>
 right=<IP addr. of the UC application computer>
 leftprotoport=%any/%any
 rightprotoport=%any/%any
 leftfirewall=no
 auto=start
 authby=secret
 keylife=1440s
 ikelifetime=3600s
 dpddelay=30
 dpdtimeout=150
 dpdaction=hold
 type=transport
 ike=aes128-sha256-modp2048
 esp=aes128-sha256-modp2048

```

- 7) Save the changes in the configuration file.
- 8) Open the following configuration file in a text editor:  
/etc/ipsec.secrets
- 9) At the end of the configuration file, define the key to be used for encrypting the MGCP data of the relevant OpenScape Media Server. This is the key you noted down during the IPsec configuration of OpenScape Voice.

In doing so, use the following format:

```

<IP addr. of the OpenScape Media Server>
<IP addr. of the MGCP interface of OpenScape Voice> :
 PSK 0x<key>

```

**Example:**

```

10.235.85.22 10.235.98.60 : PSK
 0xc3daff51c40778fe2a92f31ecb93e653
10.235.85.22 10.235.98.61 : PSK
 0xc3daff51c40778fe2a92f31ecb93e653

```

---

**NOTICE:** In the example, both MGCP connections of OpenScape Voice (10.235.98.60 / 61) end on the same

OpenScape Media Server (10.235.85.22). This is why the connections use the same key.

---

**IMPORTANT:** There must be a space between the IP-Address and the colon (":")

---



---

**NOTICE:** Leave the configuration file otherwise unchanged.

---

- 10) Save the changes in the configuration file.
- 11) Open file /etc/strongswan.conf in a text editor
- 12) Modify the file to include the following

```
strongswan.conf - strongSwan configuration file
charon
{
 # number of worker threads in charon
 threads = 16
 # plugins to load in charon
 # load = aes des sha1 md5 sha2 hmac gmp random
 pubkey xcbc x509 stroke
 plugins {
 sql
 {
 # loglevel to log into sql database
 loglevel = -1
 # URI to the database
 # database = sqlite:///path/to/file.db
 # database = mysql://user:password@localhost/
 }
 }
 database
 {
 duplicheck
 {
 # Enable duplicheck plugin (if loaded).
 # enable = yes
 enable = no
 # Whether to load the plugin. Can also be an
 integer to increase the
 # priority of this plugin. load = no
 # Socket provided by the duplicheck plugin.
 # socket = unix${piddir}charon.dck
 }
 }
}
filelog
{
/log/ipsec.log
{
add a timestamp prefix
time_format = %y%m%d-%H%M%S
prepend connection name, simplifies grepping
ike_name = yes
overwrite existing files
append = yes
increase default loglevel for all daemon
```

```

#subsystems
default = 1
flush each line to disk
flush_line = yes
}
}
 stderr
 {
 # more detailed loglevel for a specific
subsystem, overriding the
 # default loglevel.
 ike = -1
 knl = -1
 enc = -1
 net = -1
 }
...
syslog {
 # prefix for each log message
 identifier = charon
 # use default settings to log to the LOG_DAEMON
facility
 daemon {
 default = -1
 ike = -1
 enc = -1
 net = -1
 }
 # very minimalistic IKE auditing logs to
LOG_AUTHPRIV
 auth {
 default = -1
 ike = -1
 }
}
} pluto {
 # plugins to load in pluto
 # load = aes des sha1 md5 sha2 hmac gmp random
pubkey
}
libstrongswan
{
 # set to no, the DH exponent size is optimized
 # dh_exponent_ansi_x9_42 = no
}

```

- 13)** To start the IPsec service, execute the following command as root in a shell:

```
ipsec start
```

---

**NOTICE:** Every time you modify the IPSEC rules a new `ipsec restart` is necessary. With `ipsec status` or `ipsec statusall` you can check the active IPSEC Connections.

---

## IPsec Configuration

Operating System Upgrade SLES 12 SP5 or SLES 15 SP5

- 14) To have the IPsec service started automatically when the computer system of the OpenScape Media Server reboots, execute the following command as root in a shell:

```
chkconfig ipsec on
```

---

**NOTICE:** In SLES 12 installations IPsec can be enabled and started via the following commands: `systemctl enable strongswan.service` `systemctl start strongswan.service` `systemctl status strongswan.service`

---

- 15) To check whether the IPsec service works correctly, execute the following command in a shell:

```
tcpdump -i any | grep ESP
```

If OpenScape Voice and OpenScape Media Server communicate via MGCP, the shell should put out messages in the following format:

```
17:09:23.063745 IP 10.1.250.20 > adsalln1:
ESP(spi=0xf1c7d52,seq=0x16)
17:09:23.064081 IP adsalln1 > 10.1.250.20:
ESP(spi=0x39281790,seq=0x16)
17:09:23.064086 IP adsalln1 > 10.1.250.20:
ESP(spi=0x39281790,seq=0x16)
```

IPsec is now operable for MGCP connections between OpenScape Voice and OpenScape UC Application.

## 11.4 Operating System Upgrade SLES 12 SP5 or SLES 15 SP5

---

### NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
  - SLES 15 SP5, for UC V11R6
- 

After upgrading the operating system of a UC Application computer system to the corresponding SLES version, you must change the IPsec configuration of this computer system. You must use the RPM package `strongSwan`.

Consequently, you must adjust the IPsec configuration of OpenScape Voice also.

Altogether, you must execute the following steps:

- 1) [Changing the Endpoint Configuration of OpenScape Voice](#)
- 2) [Changing the IPsec Configuration of OpenScape UC Application](#)

### 11.4.1 Changing the Endpoint Configuration of OpenScape Voice

---

#### NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
- SLES 15 SP5, for UC V11R6

After upgrading the operating system of the UC Application computer systems to the corresponding SLES version, you must check and eventually change the configuration of the IPsec endpoints that connect OpenScape Voice to OpenScape UC Application in OpenScape Voice.

Change in OpenScape Voice the configuration of all IPsec endpoints concerned according to the following example:

```
Secure End Point Name <Max Length 63 (max length: 63)>
 (default:): <Unique Name for the Endpoint>
Description <Max Length 63 (max length: 63)> (default:):
FQDN <Max Length 63 (max length: 63)> (default:):
Remote IP Address < (max length: 15)> (default:): <IP
 Addr. of the UC Application Computer>
Remote NetMask < (max length: 15)> (default:):
Remote Port <0 = All Ports>:
Local Host < (max length: 32)> (default:): <for example
 csta_ip_alias_1>
Local Port <0 = All Ports>:
IPsec Profile Name <Max Length 63 (max length: 63)>
 (default:): IPSEC_ESP_SHA
IKE Profile Name <Max Length 63 (max length: 63)>
 (default:): IKE_SHA_AES
```

## 11.4.2 Changing the IPsec Configuration of OpenScape UC Application

### NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
- SLES 15 SP5, for UC V11R6

After upgrading the operating system of the UC Application computer systems to the corresponding SLES version, you must change the IPsec configuration of the UC Application computer systems concerned. Such systems are:

- The OpenScape UC Application application computer for the CSTA communication between OpenScape Voice and OpenScape UC Application. Refer to [Configuring IPsec for CSTA Connections](#) on page 692.
- For the MGCP communication between OpenScape Voice and OpenScape UC Application: Refer to [Configuring IPsec for MGCP Connections](#) on page 699.

## 12 Data Structure of the Domain Management Data

This chapter provides information about the following topics:

- [Overview of the Domain Management Data](#)
- [Accessing the Domain Management Data of a UC Application System](#)
- [Basic Structure of a CSV File](#)
- [Editing CSV Files manually](#)
- [Importing reserved Characters](#)
- [Processing a CSV File while it is being imported](#)
- [Structure of the Domain Management Data](#)

### 12.1 Overview of the Domain Management Data

The domain management data are divided among different data objects and stored in the database of a UC Application system. Each data object consists of different information organized in attributes. Each of these attributes allocates an individual database field in the database of a UC Application system.

You can access the domain management data using the import / export function of the Common Management Platform. This enables the following:

- Transmitting exported domain management data of a UC Application system to another UC Application system unchanged
- Changing exported domain management data manually and importing them in the original or in another UC Application system

The domain management data are administered outside a UC Application system in the form of a CSV file. This file contains the domain management data of a UC Application system in the form of comma-separated text lists.

### 12.2 Accessing the Domain Management Data of a UC Application System

The domain management data are stored in the database of a UC Application system. You can access them using the import / export function of the Common Management Platform.

You find detailed information about the import / export function of the Common Management Platform in the *Common Management Platform, Administrator Documentation*.

### 12.3 Basic Structure of a CSV File

A CSV file consists of different sections. Each of these sections contains the data of all objects that belong to a specific object type.

Each section is introduced by a so-called header line, which starts with the ## character string. This character string is directly followed by the name of the

respective object type and the names of the attributes available for the object type. The single names of the header line are separated by semicolon.

*Example :*

```
##User;id;domain;password;displayName;...
```

The header line is followed by single data lines with data of the single objects. Each of these lines begins with the name of the relevant object type. It is followed by the attribute values of the respective object. The object name and the single attribute values are separated by semicolon.

*Example of a data object of type User :*

```
##User; id ; domain ;password;displayName;...
User; Max ; system ;01*Test!;Max Huber;...
...
```

Which attribute a listed attribute value belongs to is determined by the sequence of the attribute names and attribute values in the data line or header line.

In the above example, the first attribute value Max belongs to the first attribute called id. The second attribute value system belongs to the second attribute called domain etc.

*Example of data objects of different object types (User and Contact):*

```
##User;id;domain;password;displayName;...
User;Max;system;01*Test!;Max Huber;...
...
##Contact;externalId;assignedSymUserIdentity;middleName;lastName;
.....
Contact;0xfffff;Max@system;Xaver;Huber;...
...
```

Because objects of selected object types are linked to each other by specific attributes, the following sequence must always be maintained in the CSV file for the sections of the different object types:

- 1) Communications systems (e.g. Switch8k)
- 2) BC Federation
- 3) Numbering plans (e.g. NPPublic)
- 4) Dial plans (e.g. DPPublic)
- 5) Telephones (e.g. Phone)
- 6) Voicemail
- 7) QueueDevice
- 8) AllocatedPhone
- 9) User
- 10) Contact
- 11) Role
- 12) ExternalId

## 12.4 Editing CSV Files manually

CSV files may exclusively be created or edited by text editors, because other programs (e. g. Microsoft Excel) may add visible or invisible characters to the actual data. Such unwanted changes may lead to CSV files being imported in a UC Application system defectively or not at all.

## 12.5 Importing reserved Characters

The following characters are reserved for internal use of the import function. Therefore, you cannot simply import them within an attribute value.

- Backslash (\)
- Hash (#)
- Semicolon (;)
- Equal sign (=)
- Comma (,)

To import one of these characters within an attribute value, it must be masked using the \-character (escape mechanism). In other words, each reserved character to be imported is prefixed with a \-character.

*Example :*

```
##OfficeCode;id;areaCode;countryCode;localOfficeCode;outsideLineInt;
outsideLineNat;overlap;attributes
OfficeCode;19\;1\#93\1;919;1;31;0;00;0;
```

is imported with the ID **19;1#93\1** as:

```
##OfficeCode;id;areaCode;countryCode;localOfficeCode;outsideLineInt;
outsideLineNat;overlap;attributes
OfficeCode;19;1#93\1;919;1;31;0;00;0;
```

## 12.6 Processing a CSV File while it is being imported

When a CSV file is imported in a UC Application system, the CSV file data are synchronized with the data already contained in the database of the UC Application system as follows:

- If the CSV file import includes an object not yet available in the database of the UC Application system, it is newly created in the database.
- If the CSV file import includes information for an object already available in the database of the UC Application system, the existing object is fully replaced with the imported object.

---

**IMPORTANT:** If the CSV file contains fewer information for an object than the associated object in the database, the additional information in the database will be lost. Therefore, import objects always with their complete information.

---



- If the database of the UC Application system includes an object for which the CSV file does not contain any information, the object in the database persists unchanged.

---

**NOTICE:** How to remove an object from the database of the UC Application system is described in [Removing Objects from the Database of the UC Application System](#) on page 717.

---

Exporting and importing data are always symmetrical processes. You can always import the data of an exported CSV file back in a UC Application system. Likewise, you can export data previously imported in the UC Application system as CSV file from the UC Application system.

However, there are the following restrictions:

- The following data cannot be exported:
  - PINs
  - Passwords
  - Values for CallForwardingDependableTarget attributes
  - Values for is8kProvisioning attributes
  - Values for phone attributes
- The following data cannot be imported:
  - Domains
  - User profiles

---

**NOTICE:** It is well possible to assign a user profile to a user by import if the relevant user profile has already been configured – e. g. in the Common Management Platform.

---

- You can import objects for OpenScape 4000 systems only once.

### Removing Objects from the Database of the UC Application System

You cannot remove objects from the database of a UC Application system by deleting them in the CSV file to be imported. In this case they persist in the database unchanged.

To remove an object from the database of a UC Application system you need to mark it as to be deleted in the CSV file to be imported. This purpose serves the deletion ID d : or D : , which you need to insert at the beginning of the relevant line.

*Example :*

```
##User;id;domain;password;displayName;...
d:User;Max;system;01*Test!;Max Huber;... \
D:User;Erika;system;02*Test!;Erika Muster;...
...
```

If the import service of the Common Management Platform finds a line marked in such a way in the CSV file, it searches the database of the UC Application system for the relevant object. If it exists in the database it is deleted; if it does not exist, the import service reports in an error message that the relevant object could not be found.

## Data Structure of the Domain Management Data

### Structure of the Domain Management Data

So that an object can be removed from the database via deletion ID you need to specify the following attributes in the given sequence directly behind the name of the relevant object type for the relevant object:

- Unique object ID (if available)
- Domain in which the object exists (if available)
- Additionally, for deleting an ExternalIdentifier object:
  - assignedUserIdentity
  - assignedExternalSystemId

*Correct examples of objects to be deleted:*

```
##NPPPrivate;id;domain;level2Code;level1Code;level0Code;switchId
d:NPPPrivate;nppprivatetest1;system;;111;00;switchtest
d:NPPPrivate;nppprivatetest2;siemens.com;;;9;switchtest2
```

```
##VoiceMail;id;domain;displayName
d:VoiceMail;+4980679999;import_export_test_domain;ourXPressionVoiceMail
```

```
##Contact;externalId;domain;middleName;lastName;givenName;displayName;
salutation;title;alias;gender;countryCode;state;postalCode;city;street;
buildingNumber;roomNumber;companyName;department;imAddress;domain;assignedPhoneNumber;assigned
assignedHomePhone;assignedSymUserIdentity
d:Contact;31107@system;system;Mirosław;Klose;Mirosław;;Herr;;;1;DE;Bayern;81379;Muenchen;Mach
+493040031107;31107@sol1.siemens.com;;;31107@system
```

```
##ExternalId;externalId;assignedUserIdentity;assignedExternalSystemId;
d:ExternalId;31107@system;gb3110@siemens.com;sametime;
```

*Incorrect example of a VoiceMail object (domain preceding id) to be deleted:*

```
##VoiceMail;domain;id
d:VoiceMail;import_export_test_domain;+4980679999
```

In a CSV file, you can combine import entries to be deleted with those to be added and updated. In doing so be sure not to delete an object still assigned to another object. In such a case the relevant object will not be deleted and an error message will point to the still existing dependency.

## 12.7 Structure of the Domain Management Data

The domain management data are divided among different data objects. Each of these data objects consists of different information organized in attributes.

You find detailed information about the single data objects of the domain management in the *OpenScape UC Application SPML SDK, Programming Guide* manual.

## 13 User Privileges for OpenScape UC Application

This chapter provides information about the following topics:

- The most important features UC Application users can deploy with the following default profiles:
  - **Essential**
  - **Professional**
  - **Team**
  - **Team Administrator**
- Hints at the selection of the default profile controlling the use of a feature in a specific UC Application client.

---

**IMPORTANT:** Whether a feature can be used in a UC Application client does normally not depend on the default profile assigned to a user. If a feature becomes accessible by an individual default profile, it is usually available in all UC Application clients that support the relevant feature. There are only few exceptions from this behavior.

---

The *OpenScape UC Application, Client Applications* manual contains a table that shows which of the most important features can be used with which of the UC Application clients.

- The privileges a UC Application user must have for deploying an individual feature.

**Table 17: User licenses and their deployable UC Application features**

| UC Application service                                      | Essential | Professional | Team | Team Administrator | Individually required privilege in the user profile |
|-------------------------------------------------------------|-----------|--------------|------|--------------------|-----------------------------------------------------|
| Call control                                                |           |              |      |                    |                                                     |
| • Make call                                                 | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Hold call                                                 | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Pick up in 1st party mode (softphone is preferred device) | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Reconnect call                                            | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Transfer (with consultation call)                         | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Consultation call                                         | ✓         | ✓            | ✓    |                    | Essential                                           |

## User Privileges for OpenScape UC Application

| UC Application service                                                                                                                               | Essential | Professional | Team | Team Administrator | Individually required privilege in the user profile |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|------|--------------------|-----------------------------------------------------|
| • Reject                                                                                                                                             | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Clear connection                                                                                                                                   | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Toggle (alternate call)                                                                                                                            | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Redialing                                                                                                                                          | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Auto-Answer (depending on the set device and as configured on the device)                                                                          | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Hot-Key click-to-call plug-in                                                                                                                      | ✓         | ✓            | ✓    |                    | Essential                                           |
| Call screening                                                                                                                                       |           |              |      |                    |                                                     |
| • Provide visual indication of incoming calls within client GUI                                                                                      | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Display caller ID and/or name of calling party                                                                                                     | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Display pop-up (including optional call features, e.g., deflect to voice mail)                                                                     | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Deflect incoming calls to voice mail on the fly                                                                                                    | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Record calls (call recording, only clients with SIP softphones)                                                                                    | ✓         | ✓            | ✓    |                    | Local Call Recording                                |
| Multiple call handling                                                                                                                               |           |              |      |                    |                                                     |
| • A user can control up to 2 calls concurrently (including conferencing on a phone)                                                                  | ✓         | ✓            | ✓    |                    | Essential                                           |
| • A user can control up to 3 calls concurrently. Including conferencing on a phone (depending on the telephone system and the set preferred device). | ✓         | ✓            | ✓    |                    | Essential                                           |

| UC Application service                                                                                                                                                          | Essential | Professional                               | Team                                          | Team Administrator | Individually required privilege in the user profile |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------------------------------------|-----------------------------------------------|--------------------|-----------------------------------------------------|
| Device handover                                                                                                                                                                 |           |                                            |                                               |                    |                                                     |
| <ul style="list-style-type: none"> <li>Users can redirect an alerting call to one of their preferred devices or any other device (e.g., mobile &lt;-&gt; desk phone)</li> </ul> | ✓         | ✓                                          | ✓                                             |                    | Essential                                           |
| <ul style="list-style-type: none"> <li>Users can redirect an active call to one of their preferred devices or any other device (e.g., mobile &lt;-&gt; desk phone)</li> </ul>   | ✓         | ✓                                          | ✓                                             |                    | Essential                                           |
| Audio conferencing – Ad-hoc                                                                                                                                                     |           |                                            |                                               |                    |                                                     |
| <ul style="list-style-type: none"> <li>Ad-hoc server-based audio conferences</li> </ul>                                                                                         |           | ✓<br>(unavailable in the voice portal)     | ✓<br>(available in the voice portal also)     |                    | Ad-hoc conference                                   |
| <ul style="list-style-type: none"> <li>User can select multiple contacts, start an Ad-hoc conference and dynamically add/remove additional participants</li> </ul>              |           | ✓<br>(unavailable in the OS Mobile Client) | ✓<br>(available in the OS Mobile Client also) |                    | Ad-hoc conference                                   |
| Audio conferencing – Meet Me                                                                                                                                                    |           |                                            |                                               |                    |                                                     |
| <ul style="list-style-type: none"> <li>Create/manage open conferences (moderatorless)</li> </ul>                                                                                |           |                                            | ✓                                             |                    | Open Conference                                     |
| <ul style="list-style-type: none"> <li>Provide a quick (self) re-join into active conference without authentication in case user dropped out by mistake</li> </ul>              |           |                                            | ✓                                             |                    | Meet Me conference                                  |
| <ul style="list-style-type: none"> <li>Create/manage moderator controlled conferences</li> </ul>                                                                                |           |                                            | ✓                                             |                    | Meet Me conference                                  |
| <ul style="list-style-type: none"> <li>Preassign other moderator(s)</li> </ul>                                                                                                  |           |                                            | ✓                                             |                    | Meet Me conference                                  |
| <ul style="list-style-type: none"> <li>Provide access number with PIN</li> </ul>                                                                                                |           |                                            | ✓                                             |                    | Meet Me conference                                  |
| <ul style="list-style-type: none"> <li>Display all conference participants (name or number) who have already joined or who are not yet in conference</li> </ul>                 |           |                                            | ✓                                             |                    | Meet Me conference                                  |

## User Privileges for OpenScape UC Application

| UC Application service                                                                                                     | Essential | Professional | Team | Team Administrator | Individually required privilege in the user profile |
|----------------------------------------------------------------------------------------------------------------------------|-----------|--------------|------|--------------------|-----------------------------------------------------|
| • Mute/unmute other participants' audio transmission                                                                       |           |              | ✓    |                    | Meet Me conference                                  |
| • Mute/unmute other participants' video                                                                                    |           |              | ✓    |                    | Meet Me conference                                  |
| • Mute conference                                                                                                          |           |              | ✓    |                    | Meet Me conference                                  |
| • Drop individual participants from conference                                                                             |           |              | ✓    |                    | Meet Me conference                                  |
| • Lock conference to block others from joining the active conference                                                       |           |              | ✓    |                    | Meet Me conference                                  |
| • Identify active speaker in the conference                                                                                |           |              | ✓    |                    | Meet Me conference                                  |
| • Enable ability to record and announce conference participant's name                                                      |           |              | ✓    |                    | Meet Me conference                                  |
| • Add document links and URLs to conference for sharing with other participants Start a web conference session             |           |              | ✓    |                    | Meet Me conference                                  |
| • Participants can select their preference ahead of time, whether they will call-in or want to be called out by the system |           |              | ✓    |                    | Meet Me conference                                  |
| • Join an active conference session without access number and PIN                                                          |           |              | ✓    |                    | Meet Me conference                                  |
| • Initiate a predefined conference session                                                                                 |           |              | ✓    |                    | Meet Me conference                                  |
| Contact list management                                                                                                    |           |              |      |                    |                                                     |
| • Manage server-based contact list stored in OpenScape                                                                     | ✓         | ✓            | ✓    |                    | Essential                                           |
| • Manage server-based contact list stored on the groupware server (Lotus Domino or Microsoft Exchange)                     | ✓         | ✓            | ✓    |                    | Essential                                           |

| UC Application service                                                                                                           | Essential                              | Professional                           | Team                                      | Team Administrator | Individually required privilege in the user profile |
|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------------------|-------------------------------------------|--------------------|-----------------------------------------------------|
| • Contact list management with search, group and sort capabilities                                                               | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| • Display contact business card, (including presence, phone number, e-mail address, location, time zone, free-form text message) | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| • Search global address books such as: corporate directories (LDAP, Lotus Domino or Microsoft Exchange)                          | ✓<br>(unavailable in the voice portal) | ✓<br>(unavailable in the voice portal) | ✓<br>(available in the voice portal also) |                    | Essential                                           |
| • Search personal contacts in groupware (LDAP, Lotus Domino or Microsoft Exchange)                                               | ✓<br>(unavailable in the voice portal) | ✓<br>(unavailable in the voice portal) | ✓<br>(available in the voice portal also) |                    | Essential                                           |
| • Import and export personal contact list                                                                                        | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| <b>Call journal</b>                                                                                                              |                                        |                                        |                                           |                    |                                                     |
| • Track incoming, outgoing, missed and forwarded calls, and calls that went to voice mail                                        | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| • Manage a server-based call journal stored on the OpenScape server                                                              | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| • Effective journal management via Search and Sort capabilities                                                                  | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| <b>One-number service (ONS)</b>                                                                                                  |                                        |                                        |                                           |                    |                                                     |
| • Direct incoming calls to user's one-number service to a "preferred" device specified by the user                               | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |
| • Send "one number" caller ID info to caller independent of user's device                                                        | ✓                                      | ✓                                      | ✓                                         |                    | Essential                                           |

## User Privileges for OpenScope UC Application

| UC Application service                                                                                                                                                                             | Essential                                  | Professional                                  | Team                                          | Team Administrator | Individually required privilege in the user profile                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------------|-----------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Manage list of “preferred” devices, incl. SIP phone, mobile phone, softphones, etc.</li> </ul>                                                              | ✓                                          | ✓                                             | ✓                                             |                    | Essential<br>(can be individually suppressed using the <b>Disable Device List Management via Client</b> privilege.) |
| <ul style="list-style-type: none"> <li>Users can set their preferred device to any other device (e.g.: a conference phone)</li> </ul>                                                              | ✓                                          | ✓                                             | ✓                                             |                    | Essential                                                                                                           |
| <ul style="list-style-type: none"> <li>Quick selection of another device to override the default preferred device for incoming and outgoing calls, and send “one number” caller ID info</li> </ul> | ✓                                          | ✓                                             | ✓                                             |                    | Essential                                                                                                           |
| OpenScope messaging                                                                                                                                                                                |                                            |                                               |                                               |                    |                                                                                                                     |
| <ul style="list-style-type: none"> <li>Ability to receive voice message and post it as an e-mail attachment in the preferred groupware inbox (Microsoft Outlook, Lotus Notes)</li> </ul>           | ✓<br>(unavailable in the OS Mobile Client) | ✓<br>(available in the OS Mobile Client also) | ✓<br>(available in the OS Mobile Client also) |                    | Voice Mail Access via ... native OpenScope Services                                                                 |
| <ul style="list-style-type: none"> <li>Quick access to voice messages via controls such as start, stop, pause, delete and save</li> </ul>                                                          | ✓                                          | ✓                                             | ✓                                             |                    | Voice Mail Access via ... native OpenScope Services                                                                 |
| <ul style="list-style-type: none"> <li>Access voice messages in a 3rd party voice mail system</li> </ul>                                                                                           | ✓                                          | ✓                                             | ✓                                             |                    | Voice Mail Access via ... a 3rd Party Voice Mail System                                                             |
| OpenScope Xpressions Integration                                                                                                                                                                   |                                            |                                               |                                               |                    |                                                                                                                     |
| <ul style="list-style-type: none"> <li>Quick access to voice messages via controls such as start, stop, pause, delete and save</li> </ul>                                                          | ✓                                          | ✓                                             | ✓                                             |                    | Voice Mail Access via ... Xpressions                                                                                |
| <ul style="list-style-type: none"> <li>Message Waiting Indication (MWI)</li> </ul>                                                                                                                 | ✓                                          | ✓                                             | ✓                                             |                    | Voice Mail Access via ... Xpressions                                                                                |
| Voice portal                                                                                                                                                                                       |                                            |                                               |                                               |                    |                                                                                                                     |



| UC Application service                                                                                                                                    | Essential | Professional | Team | Team Administrator | Individually required privilege in the user profile |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|------|--------------------|-----------------------------------------------------|
| <ul style="list-style-type: none"> <li>Select and set preferred device list via predefined device list, ANI or by entering device number</li> </ul>       | ✓         | ✓            | ✓    |                    | Voice Portal-Basic Functionality                    |
| <ul style="list-style-type: none"> <li>Manage user-defined greetings</li> </ul>                                                                           | ✓         | ✓            | ✓    |                    | Voice Portal-Basic Functionality                    |
| <ul style="list-style-type: none"> <li>Access to voice messaging management and playback functionality (depending on message system connected)</li> </ul> | ✓         | ✓            | ✓    |                    | Mailbox Access                                      |
| <ul style="list-style-type: none"> <li>Access to messages via text to speech functionality</li> </ul>                                                     | ✓         | ✓            | ✓    |                    | Email Access                                        |
| <ul style="list-style-type: none"> <li>Call contact via lookup in corporate and external directories</li> </ul>                                           | ✓         | ✓            | ✓    |                    | Dialing via Contacts                                |
| <ul style="list-style-type: none"> <li>Manage calendar appointments (listen, accept, reject, delete and forward)</li> </ul>                               | ✓         | ✓            | ✓    |                    | Calendar Access                                     |
| <ul style="list-style-type: none"> <li>Setting of user presence status</li> </ul>                                                                         |           | ✓            | ✓    |                    | Manage Presence and Rules                           |
| <ul style="list-style-type: none"> <li>Activate/deactivate rules</li> </ul>                                                                               |           | ✓            | ✓    |                    | Manage Presence and Rules                           |
| Instant Messaging                                                                                                                                         |           |              |      |                    |                                                     |
| <ul style="list-style-type: none"> <li>Enable XMPP-based IM client connections</li> </ul>                                                                 |           | ✓            | ✓    |                    | Instant Messaging                                   |
| <ul style="list-style-type: none"> <li>Multi-party IM</li> </ul>                                                                                          |           | ✓            | ✓    |                    | Instant Messaging                                   |
| <ul style="list-style-type: none"> <li>Set up a voice call from an IM session</li> </ul>                                                                  |           | ✓            | ✓    |                    | Instant Messaging                                   |
| <ul style="list-style-type: none"> <li>Set up a voice conference from an IM session</li> </ul>                                                            |           | ✓            | ✓    |                    | Instant Messaging                                   |
| <ul style="list-style-type: none"> <li>Save the current IM session</li> </ul>                                                                             |           | ✓            | ✓    |                    | Instant Messaging                                   |
| Presence                                                                                                                                                  |           |              |      |                    |                                                     |

## User Privileges for OpenScape UC Application

| UC Application service                                                                                                                                      | Essential | Professional                                                                                                                 | Team                                                                                                                            | Team Administrator | Individually required privilege in the user profile |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------|
| <ul style="list-style-type: none"> <li>Provide full spectrum display of user and telephony presence, free-form notes, and time zone info</li> </ul>         |           | <br>(unavailable in the OS Mobile Client)   | <br>(available in the OS Mobile Client also)   |                    | Presence                                            |
| <ul style="list-style-type: none"> <li>Change user presence information (user presence, free-form note, location, timezone)</li> </ul>                      |           | <br>(unavailable in the OS Mobile Client)   | <br>(available in the OS Mobile Client also)   |                    | Presence                                            |
| <ul style="list-style-type: none"> <li>OpenScape 4000-Display telephony presence</li> </ul>                                                                 |           | <br>(unavailable in the OS Mobile Client)   | <br>(available in the OS Mobile Client also)   |                    | Presence                                            |
| Rules                                                                                                                                                       |           |                                                                                                                              |                                                                                                                                 |                    |                                                     |
| <ul style="list-style-type: none"> <li>User can activate/deactivate rules</li> </ul>                                                                        |           | <br>(unavailable in the OS Mobile Client) | <br>(available in the OS Mobile Client also) |                    | Rules                                               |
| <ul style="list-style-type: none"> <li>Create/manage simple call routing table based on presence status</li> </ul>                                          |           | <br>(unavailable in the OS Mobile Client) | <br>(available in the OS Mobile Client also) |                    | Rules                                               |
| <ul style="list-style-type: none"> <li>Create and manage rules simplified</li> </ul>                                                                        |           | <br>(unavailable in the OS Mobile Client) | <br>(available in the OS Mobile Client also) |                    | Rules                                               |
| <ul style="list-style-type: none"> <li>Rule attributes can include elements such as: originator, date &amp; time, presence status, devices lists</li> </ul> |           | <br>(unavailable in the OS Mobile Client) | <br>(available in the OS Mobile Client also) |                    | Rules                                               |
| <ul style="list-style-type: none"> <li>Assign rule names</li> </ul>                                                                                         |           | <br>(unavailable in the OS Mobile Client) | <br>(available in the OS Mobile Client also) |                    | Rules                                               |
| Web conferences                                                                                                                                             |           |                                                                                                                              |                                                                                                                                 |                    |                                                     |
| <ul style="list-style-type: none"> <li>Schedule a web conference</li> </ul>                                                                                 |           |                                                                                                                              | <br>(available in the OS Mobile Client also) |                    | Web Collaboration                                   |
| <ul style="list-style-type: none"> <li>Conduct and moderate a web conference</li> </ul>                                                                     |           |                                                                                                                              | <br>(available in the OS Mobile Client also) |                    | Web Collaboration                                   |
| Video                                                                                                                                                       |           |                                                                                                                              |                                                                                                                                 |                    |                                                     |

## User Privileges for OpenScape UC Application

| UC Application service                                                                                                                                | Essential | Professional | Team | Team Administrator | Individually required privilege in the user profile |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------------|------|--------------------|-----------------------------------------------------|
| <ul style="list-style-type: none"> <li>Initiate a video call with another OpenScape Personal or OpenScape Enterprise SIP softphone station</li> </ul> | ✓         | ✓            | ✓    |                    | Essential                                           |
| <ul style="list-style-type: none"> <li>Initiate point-to-point connection with an OpenScape video station</li> </ul>                                  | ✓         | ✓            | ✓    |                    | Essential                                           |
| Team function                                                                                                                                         |           |              |      |                    |                                                     |
| <ul style="list-style-type: none"> <li>Form and manage teams of OpenScape users</li> </ul>                                                            |           |              |      | ✓                  | Symphonia Group Management                          |
| <ul style="list-style-type: none"> <li>Each team member is notified about calls that arrive for other members of the same team</li> </ul>             | ✓         | ✓            | ✓    |                    | Essential                                           |
| <ul style="list-style-type: none"> <li>Each team member can answer calls that arrive for other members of the same team</li> </ul>                    | ✓         | ✓            | ✓    |                    | Essential                                           |
| <ul style="list-style-type: none"> <li>Each team member can also see the call journals of the other members of the same team</li> </ul>               | ✓         | ✓            | ✓    |                    | Essential                                           |
| <ul style="list-style-type: none"> <li>Release of team-wide display of calls and call journal</li> </ul>                                              | ✓         | ✓            | ✓    |                    | Essential                                           |

## 14 Voice Portal Settings in the CMP (Voice Portal Plug-in)

This chapter provides information about the following topics of the voice portal plug-in:

- [Function of the Voice Portal Plug-in](#)
- [Opening the Voice Portal Plug-in](#)
- [Configuring Application Profiles](#)
- [General Application Profile Settings](#)
- [Mailbox Settings of Application Profiles](#)
- [Special Language Settings of Application Profiles](#)
- [Call Settings of Application Profiles](#)
- [Operation Mode Settings of Application Profiles](#)

### 14.1 Function of the Voice Portal Plug-in

You can perform the settings of the voice portal applications **Voice Portal** and **Voice Portal Speech** specific to the Media Server in the voice portal plug-in of the CMP. This configuration is based on voice portal application profiles. Using a terminal you can bind each of these application profiles to access numbers, thus realizing voice portal accesses with individual settings.

### 14.2 Opening the Voice Portal Plug-in

How to open the voice portal plug-in of the CMP:

1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.

2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

5) Select in the list the link of the voice portal application for which you wish to configure a user access.

- Select the **Voiceportal** application, if you wish to configure a user access controlled via telephone keys.
- Select the **Voiceportalspeech** application, if you wish to configure a voice-controlled user access.

The configuration dialog of the voice portal plug-in opens. You see a list of all application profiles configured in the selected OpenScape Media Server for the selected voice portal application.

## 14.3 Configuring Application Profiles

The voice portal applications support two types of application profiles:

- Profile type **Voice Portal access** This profile type specifies the settings for the user accesses of the voice portal applications.
- Profile type **Guest Portal access** This profile type specifies the settings for the user accesses of the voice portal applications.

For the voice portal applications of each OpenScape Media Server an application profile has already been pre-configured for each profile type:

- Application profile **start** for the profile type **Voice Portal access**.
- Application profile **guest** for the profile type **Guest Portal access**.

**Voice Portal Speech Configuration**

Administer the Voice Portal Speech Application Configuration

**General Application Configuration**

Task to create the grammars **Execute...**

**Profile Configuration**

**Profiles**

|                       |                             |   |
|-----------------------|-----------------------------|---|
| <input type="radio"/> | start (Voice Portal access) | ▶ |
| <input type="radio"/> | guest (Guest Portal access) | ▶ |

Close

The application profiles overview provides the following buttons:

### Execute

Creates the grammars for the speech recognition of the application Voiceportalspeech.

---

**NOTICE:** This button is only available for the application Voiceportalspeech.

---

### Copy

Opens the configuration dialog for a new application profile. The profile type and default settings correspond to those of the application profile selected in the profile list.

### Edit

Opens the configuration dialog for the application profile selected in the profile list.

Remove

Deletes the application profile selected in the profile list. The pre-configured application profiles **start** and **guest** cannot be deleted.

14.3.1 Profile Settings for Profile Type Voice Portal Access

The settings of an application profile of type **Voice Portal access** are divided in the following areas:

- General settings
- Mailbox settings
- Special language settings
- Call settings
- Operation mode

**NOTICE:** This section is available for the voice portal application only.

14.3.2 Profile Settings for Profile Type Guest Portal Access

The settings of an application profile of type **Guest Portal access** are divided in the following areas:

- General
- Mailbox settings

14.4 General Application Profile Settings

On the **General** tab of the profile settings you configure basic settings for the voice portal access that uses the relevant application profile.

General Settings

Voice Portal Speech default language:

English (United States)

Symphonia domain:

system

Address translation context:

DefaultContext

Enforce name recording (on login):

☐

Enable direct conference access after login:

☒

Default language

|          |              |
|----------|--------------|
| Default: | English (US) |
|----------|--------------|

|                         |                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Possible values:</i> | <ul style="list-style-type: none"> <li>• German</li> <li>• English (UK)</li> <li>• English (US)</li> <li>• Spanish</li> <li>• French</li> <li>• Italian</li> <li>• Portuguese (Brazil)</li> <li>• Portuguese (Portugal)</li> <li>• Chinese</li> </ul> |
| <i>Remark:</i>          | Only those languages are offered for selection that have been installed for the language package.                                                                                                                                                     |

The voice portal always plays the first announcements in a language that is independent from the calling user – this is the so-called default language.

Only after the calling user has logged in to the voice portal, the portal tries to determine the user-individual language setting. To do this, it searches in the OpenScape user database for the individual user settings based on the logon data used. If the determined user-individual language setting is different from the default setting, the voice portal switches the TUI to the language determined.

To guests, the voice portal announcements can only be played in the default language.

**Default language** defines the default language for the voice portal access.

#### Symphonia domain

|                 |                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Default:</i> | system                                                                                                                                                                 |
| <i>Remark:</i>  | <ul style="list-style-type: none"> <li>• Cannot be modified.</li> <li>• Can only be configured for application profiles of type <b>Voice Portal access</b>.</li> </ul> |

#### Address translation context

|                         |                                         |
|-------------------------|-----------------------------------------|
| <i>Default:</i>         | –                                       |
| <i>Possible values:</i> | <ID of an address translation context > |

If e.g. a user needs to specify a phone number in the voice portal, he/she will do this always with reference to the respective location. For example, as pure extension or as phone number with area code but without international prefix. But this leads to problems if the voice portal e.g. is located in a country different from the user's.

To evade such phone number problems, the OpenScape system transforms all phone numbers before the actual processing into a normalized phone number format – e. g. +492404901100. The thus normalized phone numbers then contain all information that the phone number uniquely identifies or localizes.

The OpenScape system uses so-called address translation contexts for phone number normalization.

If an OpenScape user enters a phone number via the voice portal TUI, the voice portal uses the information of the relevant OpenScape user as address translation context. If this is not possible, the voice portal uses address translation contexts that can be configured in the CMP instead.

**Address translation context** defines the ID of an address translation context configured in the CMP. The voice portal uses this context for phone number normalization, if no OpenScape user is available as address translation context.

### First redirected number of the list

|                |                                                                                      |
|----------------|--------------------------------------------------------------------------------------|
| <i>Remark:</i> | Can only be configured for application profiles of type <b>Guest Portal access</b> . |
|----------------|--------------------------------------------------------------------------------------|

If a call that has been forwarded several times is handed over to the voice portal, the voice portal can use one of two phone numbers as originator number:

- The phone number from which the call was forwarded initially.
- The phone number from which the call was forwarded for the last time.

If the option **First redirected number of the list** is active, the voice portal uses the phone number as originator number from which the call was forwarded initially.

If the option **First redirected number of the list** is inactive, the voice portal uses the phone number as originator number from which the call was forwarded the last time.

### Maximal number of private contacts

|                         |                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------|
| <i>Default:</i>         | 100                                                                                          |
| <i>Possible values:</i> | <1 ... 100>                                                                                  |
| <i>Remark:</i>          | Can only be configured for application profiles of the <b>Voiceportalspeech</b> application. |

The voice portal TUI allows users to enter global voice commands for any menu option. Such global voice commands can also contain private OpenScape contacts that the TUI speech recognition tries to recognize.

**Maximal number of private contacts** determines how many private OpenScape contacts the TUI speech recognition considers for recognizing global voice commands at the most. If an OpenScape user manages more private OpenScape contacts than are specified in **Maximal number of private contacts**, recognizing spoken OpenScape contacts may fail.

Greater values for **Maximal number of private contacts** mean worse quality of contact recognition.

### Enforce name recording (on login)

|                |                                                                                      |
|----------------|--------------------------------------------------------------------------------------|
| <i>Remark:</i> | Can only be configured for application profiles of type <b>Voice Portal access</b> . |
|----------------|--------------------------------------------------------------------------------------|



Determines whether a user needs to record a name announcement after his/her first login at the voice portal user access. The voice portal uses the name announcement when the name of the relevant user is played in the TUI.

#### Enable direct conference access after login

|                |                                                                                                                                                |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Remark:</i> | Can only be configured for application profiles of type <b>Voice Portal access</b> that are configured for the <b>Voiceportal</b> application. |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|

After an OpenScape user has dialed into the voice portal, the main menu is played to him/her by default.

If **Enable direct conference access after login** is active and there is at least one active conference for the user, he/she is offered to enter one of the relevant conference rooms instead. Only if the user refuses to enter the conference room the main menu is played.

## 14.5 Mailbox Settings of Application Profiles

On the **Mailbox Settings** tab of the profile settings you configure the mailbox settings for the voice portal access that uses the relevant application profile.

**Mailbox Settings**

---

Use subject suffix for voice mails: ☐

Subject suffix for voice mails:

#### Use subject suffix for voice mails

When the voice portal sends a voice message to an OpenScape user, you can suffix the message's subject with a fixed text.

**Use subject suffix for voice mails** activates this feature.

#### Subject suffix for voice mails

|                         |                                                             |
|-------------------------|-------------------------------------------------------------|
| <i>Default:</i>         | Example text for message subject line suffix to be replaced |
| <i>Possible values:</i> | <Text>                                                      |

When the voice portal sends a voice message to an OpenScape user, you can suffix the message's subject with a fixed text.

**Subject suffix for voice mails** defines the text that is attached to the subject of the voice message. This requires the option **Use subject suffix for voice mails** to be active.

## 14.6 Special Language Settings of Application Profiles

Using the text-to-speech feature of the voice portal, users can have texts read out. In this process the system can automatically optimize the voice output by analyzing the message text sentence-wise and using the text-to-speech engine for the recognized language.

**NOTICE:** You can perform the language settings only for application profiles of type **Voice Portal access**.

On the **Special Language Settings** tab you select the languages for which the text-to-speech feature analyzes message texts.

Language Detector Settings

Sel:3 | Items/Page: 10 | All:7

☐

Languages which should be used for the language recognizer feature (to read e-mails)

|                                     |                                                                                     |            |
|-------------------------------------|-------------------------------------------------------------------------------------|------------|
| <input checked="" type="checkbox"/> |    | English    |
| <input checked="" type="checkbox"/> |    | German     |
| <input type="checkbox"/>            |    | Spanish    |
| <input type="checkbox"/>            |    | French     |
| <input type="checkbox"/>            |    | Italian    |
| <input type="checkbox"/>            |   | Portuguese |
| <input checked="" type="checkbox"/> |  | Chinese    |

## 14.7 Call Settings of Application Profiles

On the **Call Settings** tab you configure settings that determine the call behavior of the voice portal access that uses the relevant application profile.

**NOTICE:** You can perform the call settings only for application profiles of type **Voice Portal access**.

Call Settings

Operator number:

0

Transfer timeout (in seconds):

30

### Operator number

|                  |                |
|------------------|----------------|
| Default:         | 0              |
| Possible values: | <phone number> |

This phone number is dialed when the user enters 00 in the voice portal main menu.

### Transfer timeout

|                         |                  |
|-------------------------|------------------|
| <i>Default:</i>         | 30 [second]      |
| <i>Possible values:</i> | <time> [seconds] |

Specifies how long the system attempts to reach the dialed phone number in case of a forwarding. If the forwarded call is not accepted at the forwarding destination within the specified period, the voice portal cancels the forwarding.

## 14.8 Operation Mode Settings of Application Profiles

On the **Operation Mode** tab you configure special operation modes for the voice portal access that uses the relevant application profile.

**NOTICE:** You can perform the call settings only for application profiles of type **Voice Portal access**.

| <b>Third Party Mode</b>                                          |                                |                                   |                                |                                |      |          |
|------------------------------------------------------------------|--------------------------------|-----------------------------------|--------------------------------|--------------------------------|------|----------|
| Third Party Voice Mail Number:                                   |                                | <input type="text" value="4711"/> |                                |                                |      |          |
| <b>Xpressions Mode</b>                                           |                                |                                   |                                |                                |      |          |
| Xpressions Number:                                               |                                | <input type="text" value="4712"/> |                                |                                |      |          |
| Trusted Transfer Domain:                                         |                                | <input type="text" value="49"/>   |                                |                                |      |          |
| <b>Xpression Parameter Configuration (Number of characters):</b> |                                |                                   |                                |                                |      |          |
| Items/Page: 10   All: 1                                          |                                |                                   |                                |                                |      |          |
| Signaling                                                        | Domain                         | Direction                         | ANI                            | Account number                 | Menu | Language |
| 1                                                                | <input type="text" value="2"/> | 1                                 | <input type="text" value="4"/> | <input type="text" value="4"/> | 2    | 1        |

### Third Party Voice Mail Number

|                         |                |
|-------------------------|----------------|
| <i>Default:</i>         | 4711           |
| <i>Possible values:</i> | <phone number> |

If you integrate the voicemail system of a third-party supplier in OpenScape UC Application, you need to specify the access number for the relevant voicemail system here.

### Xpressions Number

|                         |                |
|-------------------------|----------------|
| <i>Default:</i>         | 4712           |
| <i>Possible values:</i> | <phone number> |

If you connect the voice portal to an XPR server via the Trusted Transfer Mode, you need to specify the access number for the XPR PhoneMail script here.

### Trusted Transfer Domain

|                         |                     |
|-------------------------|---------------------|
| <i>Default:</i>         | 49                  |
| <i>Possible values:</i> | <TTM domain number> |

Specifies the ID of the trusted domain that is or will be configured in the XPR system as local trusted domain. If the voice portal receives a forwarded TTM call from the XPR server, it checks the domain ID forwarded with the call. If this forwarded domain ID does not correspond to the one configured here, the call will be rejected as unauthorized.

### Xpressions Parameter Configuration

Defines the calling number schema for an OpenScape Xpressions connection.

---

**NOTICE:** As of OpenScape Xpressions V7 R1 the XPR server uses value **2** for the **Voice** setting in the calling number schema. This value cannot be changed. Therefore, value **2** must always be set under **Voice** when the voice portal is connected to an XPR server via the Trusted Transfer Mode.

---

If a user is forwarded to the XPR server via the Trusted Transfer Mode of OpenScape UC Application or vice versa, various information must be exchanged between OpenScape UC Application and the XPR server with the forwarding. The calling number schema specifies in which format this information is exchanged.

You find further information about the calling number schema in [Calling Number Schema](#) on page 37.

## 15 Conference Portal Settings in the CMP (Conference Portal Plug-in)

This chapter provides information about the following topics and settings of the conference portal plug-in:

- [Function of the Conference Portal Plug-in](#)
- [Conference Management](#)
- [Number configuration](#)
- [Configuration](#)
- [Media Configuration](#)
- [Other Settings](#)

### 15.1 Function of the Conference Portal Plug-in

---

**NOTICE:** All terminal-individual settings in the conference portal plugin affect only the **conferencing-default** terminal of the existing OpenScape Media Servers.

---

The most important conference portal settings can be configured for all Media Servers in the CMP conference portal plugin. Further configurations are performed as usual via the configuration dialogs of the existing OpenScape Media Servers.

How to access the CMP conference portal plugin:

- 1) Click on the **Unified Communications** menu item on the **Configuration** navigation tab of the CMP.
- 2) In the navigation tree, click on **Configuration > Conferences**.

The configuration dialog of the conference portal plugin opens.

The conference portal plugin settings are divided into the following tabs:

- **Conference management**
- **Configuration**
  - **Configuration**
  - **Number configuration**
  - **Media configuration**
  - Other settings

### 15.2 Conference Management

You can search the conference portal plug-in for created conferences by selected criteria and change their settings to some degree.

Conference Portal Settings in the CMP (Conference Portal Plug-in)

Mode: 

Created Conferences

Type: 

All

Invitees: 

Creator

Schedule time: 

between 5/17/13 and 5/17/13

Conference Origin-ID:

Update list

Reassign...

Activate Video...

Delete...

Sel:0 | Items/Page: 10 | All:0

| <div></div> | Creator              | Subject | Schedule time | Media       | Status |
|-------------|----------------------|---------|---------------|-------------|--------|
| <div></div> | administrator@system | Video 2 | not planed    | <div></div> |        |

Mode

Specifies the mode for finding conferences configured in the conference portal. You can choose from the following modes:

- Created Conferences
- Active Conferences

You can use 

->

 to toggle the modes.

Depending on the configured mode, the following search criteria are available for displaying conferences:

| Created Conferences                                                                                                                     | Active Conferences                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• <b>Type</b></li><li>• Invitees</li><li>• Schedule time</li><li>• Conference Origin-ID</li></ul> | <ul style="list-style-type: none"><li>• Participants</li><li>• Conference Origin-ID</li></ul> |

Type

Specifies a type to act as criterion for searching available conferences. This setting is only available if you have selected **Created Conferences** under **Mode**.

Possible settings are:

|                                                                                                                                                                                         |                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• <b>All</b></li><li>• <b>Scheduled for Today</b></li><li>• <b>Scheduled for next 3 Days</b></li><li>• <b>Scheduled for next 7 Days</b></li></ul> | <ul style="list-style-type: none"><li>• <b>Scheduled for next 30 Days</b></li><li>• <b>Scheduled for time interval</b></li><li>• <b>Not scheduled</b></li><li>• <b>orphaned</b></li></ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Invitees

Specifies an OpenScope user as search criterion. The available conferences are filtered by the specified OpenScope user having been invited for the

respective conference. If you wish to filter only conferences the specified OpenScape user has created, enable the **Creator** option. This setting is only available if you have selected **Created Conferences** under **Mode**.

---

**NOTICE:** The creator of a MeetNow! conference is the OpenScape user who dials into the conference first. For all other conference types the creator is the OpenScape user who creates or initiates the relevant conference in his/her OpenScape client.

---

### Participants

Specifies an OpenScape user as search criterion. The available conferences are filtered by the specified OpenScape user having dialed into the respective conference. If you wish to filter only conferences of which the specified OpenScape user is the dialed-in creator, enable the **Creator** option. This setting is only available if you have selected **Active Conferences** under **Mode**.

---

**NOTICE:** The creator of a MeetNow! conference is the OpenScape user who dials into the conference first. For all other conference types the creator is the OpenScape user who creates or initiates the relevant conference in his/her OpenScape client.

---

### Schedule time between ... and ...

Specifies a period as search criterion. The available conferences are filtered by their respective start time being within the specified period. This setting is only available if you have selected **Created Conferences** under **Mode**.

### Conference Origin-ID

Specifies a client ID as search criterion. The available conferences are filtered by the respective conference having been created in the selected OpenScape client.

### Update list

Starts the search for all conferences that meet the specified search criteria. The search hits are displayed as list in the dialog. To select the relevant conference, enable the radio button that precedes the associated list entry. You can then change the conference's settings to some degree. See [Reassign](#), [Activate Video](#), [Delete](#) and [Terminate](#).

### Reassign

If you remove an OpenScape user account from the user database of OpenScape UC Application that has been entered as conference creator, so-called orphaned conferences are the consequence. Compare [Automatic cleanup of conferences after system user deletion](#). The **Reassign** option allows assigning a new OpenScape user account to orphaned conferences as creator. This setting is only available if you have selected **Created Conferences** under **Mode**.

### Activate Video

Activates video-compatibility for the selected conferences. This setting is only available if you have selected **Created Conferences** under **Mode**.

---

**NOTICE:** Video-compatibility as such is not an indication of a conference actually using Video. Devices that exclusively use Audio but no Video may thus dial into a video-compatible conference. In this case, the relevant conference is still video-compatible, but no video composer that processes video information and transmits it to the devices is started in the conference portal.

---

### Delete

Deletes the selected conferences irretrievably. This setting is only available if you have selected **Created Conferences** under **Mode**.

### Terminate

Terminates the selected conferences. This setting is only available if you have selected **Active Conferences** under **Mode**. Configuration

## 15.2.1 Conference settings

### Maintenance Time

Sets the time to run the maintenance in HH:MM format, e.g. 02:00.

Sets the time period to keep the terminated conferences in months, weeks or days.

### User Resolving

Configures the context for the call-in number normalization, i.e. the address translation context.

Sets the context domain for user resolving, e.g. system.

### Miscellaneous settings

Selects whether the cleanup of conferences will be automatic after user deletion.

## 15.2.2 DTMF settings

Opens the configuration dialog to configure the settings for the DTMF-based conference control.

Conference participants can control selected functions of the conference portal by using their phone keypad.



### General settings for audio and video conferences

- **Disable DTMF menu in conference room**

*Default:* disabled

Defines if conference participants may control selected functions of the conference portal by using their phone keypad. If the [Disable DTMF menu in conference room](#) option is not activated, conference participants can control the following functions by pushing the phone keys assigned to each function:

---

**NOTICE:** Some of the following functions can possibly only be controlled by selected conference participants. You find detailed information in the *OpenScape UC Application, Client Applications* manual.

---

- **Prompt menu**

*Default:* \*\*

If a conference participant selects this option, all control options for the conference portal functions are played.

- **Lock conference**

*Default:* \*2

If a conference participant selects this option, no further participants will be able to log in to the conference. Selecting this option once more lifts the dial-in lock again.

- **Mute self**

*Default:* \*3

If a conference participant selects this option, the conference portal will mute him/her. The conference participant will only be able to hear the other conference participants, but will not be heard by the other conference participants. If the conference participant selects this option anew, he will be heard by the other conference participants again.

- **Mute conference**

*Default:* \*4

If a conference participant selects this option, the conference portal will mute all other conference participants. Only this conference participant will be heard by the other conference participants. If afterward another conference participant selects this option, the relevant conference participant will also be heard again.

- **Initiate device handover**

*Default:* \*5

If a conference participant selects this option, he/she will be able to change the device he uses to participate in the conference.

- **Toggle music on hold**

*Default:* \*9

If a conference participant selects this option, he/she deactivates the conference portal's music-on-hold for himself/herself.

- **Enter moderator PIN**

*Default: \*6*

If a conference participant selects this option, he/she selects to enter the moderator's PIN in order to access the conference as a moderator.

- **Start/pause recording**

*Default: \*7*

If a conference participant selects this option, he/she selects whether the recordings can be stopped or paused.

### 15.2.3 DTMF Video

DTMF video settings for video conferences

---

**IMPORTANT:** Key combination **00** is the permanent default for showing the video menu on the device display. This combination cannot be changed. To avoid allocating key combination **00** for other purposes is must not be used for any of the following DTMF settings.

---

- **Show participant list**

*Default: 88*

If a conference participant selects this option, he/she sees the list of video conference participants on the device display. If a conference participant selects this option once more, the list of video conference participants is hidden.

- **Info status on / off**

*Default: 87*

If a conference participant selects this option, he/she sees the info status on the device display. If a conference participant selects this option once more, the info status is hidden.

The info status shows e.g.:

- Allocated bandwidth for data transmission from the Media Server to the device.
- Number of participants dialed into the conference.
- Muting status

- **Switch to 'Tile' based layout**

*Default: 89*

If the conference participant selects this option, he/she sees the conference participants in video images of the same size (tile-base layout).

- **Switch to the 'Active Speaker' layout**

*Default: 86*

If the conference participant selects this option, he/she sees the respectively active speaker in a larger video image; all other conference participants appear in smaller video images of the same size.

As a rule, the image of this active speaker reacts to a change of the person who conducts the conversation slightly delayed. This prevents the image of the active speaker from changing too often.

- **Switch to the Single layout**

*Default: 85*

If a conference participant selects this option, all other conference participants see only the image of the currently speaking conference participant.

As a rule, the image of this active speaker reacts to a change of the person who conducts the conversation slightly delayed. This prevents the image of the active speaker from changing too often.

- **Switch to the Presentation layout**

*Default: 82*

If a conference participant selects this option, the presentation layout is displayed.

- **Toggle Self View**

*Default: 84*

If a conference participant selects this option, his/her own video image is suppressed on his/her device display. If the conference participant select this option once more, he/she sees their own video image.

## 15.2.4 Timer settings

Settings for Telephone User Interface (TUI)

In this section, you can configure the conferencing forerun period, during which the participants can join the conference.

### Conference forerun period

*Default: 300 [seconds]*

*Possible values: <time> [seconds]*

Participants can already dial into a conference before the scheduled conference start. [Conference forerun period](#) specifies the duration of this dial-in period.

### Conference grace period

*Default: 60 [seconds]*

*Possible values: <time> [seconds]*

Defines a grace period for terminating a conference.

If the criterion that ends a conference occurs, there is still the configured grace period for the conference to stay active. The conference is not definitely

terminated until the grace period has expired and the criterion for ending the conference is still valid.

Criteria for ending a conference are:

- For open conferences: The last user logs off
- For moderated conferences: The last moderator logs off

### Call-out ring timeout

*Default:* 30 [seconds]

*Possible values:* <time > [seconds]

The conference portal can call participants at the start of a conference to integrate them in the conference. For such a call, [Call-out ring timeout](#) defines how long the conference portal waits for the callee to accept the call. If the callee does not accept the call within this period, the conference portal cancels the call without integrating the callee in the conference.

### Rejoin grace period

*Default:* 5 [minutes]

*Possible values:* <time > [minutes]

A conference participant may have to leave a conference unintentionally – e. g. because the telephone connection is cut. If such a conference participant rejoins the conference within a specific period, he/she is automatically connected to his/her previous conference without having to make any further entries.

[Rejoin grace period](#) specifies within which period a conference participant is automatically reconnected to his/her previous conference. You can set the following parameters:

- Maximum duration for a conference in minutes.
- Autoprolong conferences provided that resources are available.
- The prolong time in minutes in case "Autoprolong is enabled."

### Maximum Conference Duration

*Default:* 720 [minutes]

*Possible values:* <Duration> [minutes]

*Remark:* Optional

Specifies the maximum time a conference may last for being prolonged automatically. Make this specification in minutes. If a conference's duration reaches the value specified here, it cannot be automatically prolonged any further. If a prolonged duration has already been defaulted at the conference start, this prolonged conference duration applies. Such a conference is generally not automatically prolonged though. To prolong a conference automatically, the [Auto-Prolong On](#) setting must be active also.

### Auto-Prolong On

*Default:* active

Specifies whether conferences can be automatically prolonged when the end of the scheduled conference duration is reached but conference participants are still logged in. Appropriate system resources must be available in the

conference portal for a conference to be prolonged. Whether a conference is actually prolonged depends on the [Maximum Conference Duration](#) setting also.

### **Prolong time**

*Default:* 30 [minutes]

*Possible values:* <Duration> [minutes]

Specifies the period a conference can be automatically prolonged by when the end of the scheduled conference duration is reached but conference participants are still logged in. Appropriate system resources must be available in the conference portal for a conference to be prolonged. Whether a conference is actually prolonged depends on the [Maximum Conference Duration](#) setting also.

### **Time**

*Default:* every Sunday

*Possible values:*

- Daily
- Hourly
- every Monday
- every Tuesday
- every Wednesday
- every Thursday
- every Friday
- every Saturday
- every Sunday

Specifies on which weekday or at which hour the conference service shall start maintenance automatically. During maintenance work, reservations of unused conferences are deleted.

### **at**

*Default:* 02:00

*Possible values:*

- <Hour in the format <hh>:<mm> > [o' clock]
- <minute(s) in the format <mm>>

Specifies the exact time at which the conference service shall automatically start its maintenance works. The following applies:

- If the option selected under [Time](#) refers to a day, you need to specify an hour under [at](#). This is then the hour at which maintenance works start on the selected day.
- If option **Hourly** is selected under [Time](#), you need to specify minutes under [at](#). This is then the minute at which maintenance works start every hour.

## **15.3 Number configuration**

### 15.3.1 Bridge numbers

In this section, you can select the Tenant ID/Numbering Plan and manage additional bridge numbers for that Tenant ID. Tenant IDs are used to generate the "Additional numbers" area in e-mail notifications.

"Use for callouts" can be used as the caller ID in callouts.

You can define toll numbers, toll free numbers or additional numbers

*Default:* –

*Possible values:* <phone number>

---

**NOTICE:** Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

---

You can define the phone number used as originator address when the conference portal initiates a call or sends an e-mail. If you use a stand-alone OpenScape Media Server, specify here the phone number entered under [Bridge Numbers – Media Server Selection](#). If you use a Media Server farm, specify here one of the phone numbers equally configured on all OpenScape Media Servers as additional phone number (cf. [list of all additional phone numbers](#) >).

Several phone numbers must be separated by a semicolon followed by a blank.

*Example:* Germany: +49 2404 901100; USA: +1 241 901100

### 15.3.2 Trunk numbers

You can configure the numbers that match the conferencing application in Media Server. The Media Server portlet must be used for an extended configuration of the terminals. In case of an installation with several Media Server nodes the main number for the node is equal to its unique trunk number on the PBX. The central bridge number can be configured under Additional numbers.

---

**IMPORTANT:** The field Trunk Number must not be empty, else problems with Conferences could appear.

---

Number configuration for Media Server nodes

Displays for all OpenScape Media Servers the configured default language access numbers for the conference portal – thus all conference portal accesses that use the language selected under [Default language](#) as default language.

In the **Number** column you see the phone number configured for the relevant OpenScape Media Server under [Bridge Numbers – Media Server Selection](#). This must always be a phone number specific to the Media Server.

The **Additional numbers** column displays are additional phone numbers of the relevant OpenScape Media Server. In case of a Media Server farm this is at least one phone number that must be the same for all Media Servers of the Media Server farm. When you click on the link of a listed Media Server node,

you open the configuration dialog for the associated conference portal. In this configuration dialog you can perform the following settings:

- [Bridge Numbers – Media Server Node Configuration](#)
- [Bridge Numbers – Media Server Selection](#)

### 15.3.3 Language dependent bridge numbers

Opens a dialog in which you can configure conference portal accesses using a default language different from the one selected under [Default language](#) for all OpenScape Media Servers. Enter the new number, click Update and then Save. You can also remove numbers by selecting the required number and clicking Remove.

---

**NOTICE:** In the Media Server configuration, language dependent bridge numbers are bound to the associated Media Server application **Conferencing#welcome\_<language token>** via the respective language-individual terminal **conferencing-<language token>**. Language dependent bridge numbers thus support merely the language as default language that results from the language token. If you wish to configure conference portal accesses that always use the language selected under [Default language](#) as default language, you need to configure the phone numbers desired for this purpose as additional phone number (cf. [<list of all additional phone numbers>](#)).

---

## 15.4 Configuration

In the conference portal plugin you can configure the following phone numbers for accessing the conference portal.

### 15.4.1 Bridge Numbers – Media Server Node Configuration

*Default:* –

*Possible values:* <phone number>

---

**NOTICE:** Always specify the phone numbers in the format in which they are sent from the communications system to the OpenScape Media Server during the connection setup.

---

Defines the phone number under which the conference portal of the relevant OpenScape Media Server can be reached. This conference portal access always uses the language selected under [Default language](#) as default language. If you use a Media Server farm, this is the Media-Server-individual phone number of the relevant OpenScape Media Server.

**max. number of participants**

*Default:* 200

Defines the maximum number of participants admitted to each conference of the relevant OpenScape Media Server.

### **<list of all additional phone numbers >**

Displays the phone numbers of the conference portal accesses that, like the [Bridge Numbers – Media Server Selection](#), also use the default language selected under [Default language](#). If you want to create an additional phone number not only on the OpenScape Media Server the settings of which are currently displayed, but also on all other OpenScape Media Servers of a Media Server farm, the entry **Yes** is displayed under **Create on all nodes**. To select the relevant additional phone number, enable the check box that precedes the associated list entry. Subsequently, you can remove the additional phone number for the relevant OpenScape Media Server. See [Remove](#).

---

**NOTICE:** If you use a Media Server farm, an additional phone number must be configured in each OpenScape Media Server of this Media Server farm. This phone number must be the same for all OpenScape Media Servers. Specify this additional phone number under Toll number also.

---

### **Create on all nodes**

If this option is active when you select [Add](#), the phone number from **New number** is added on all OpenScape Media Servers of the UC Application system or of the UC Application cluster. In this case, the list of additional phone numbers displays entry **Yes** in the table column **Create on all nodes** for the relevant phone number.

### **Add**

Adds to the list of additional phone numbers the phone number specified under **New number**.

---

**NOTICE:** In the Media Server configuration, additional phone numbers are bound to the Media Server application **Conferencing#welcome** via the **conferencing-default-addnumbers** terminal. Additional phone numbers thus support exclusively the default language selected under [Default language](#). If you wish to configure conference portal accesses for further default languages, you need to configure the desired phone numbers under [Language dependent bridge numbers](#).

---

### **Remove**

Deletes all selected phone numbers in the list of additional phone numbers.

## 15.4.2 Bridge Numbers – Media Server Selection

In the conference portal plug-in you can determine for an OpenScape Media Server which conference services to provide and for which users.

### **Media support**

*Default:*



- Audio only
- Video

*Possible values:*

- Audio only – pure audio conferences and no video-compatible conferences are supported
- Video – video-compatible conferences and no pure audio conferences are supported

Defines which type of conferences the relevant OpenScape Media Server provides. You can activate the possible options individually or combined.

---

**NOTICE:** MeetNow! conferences are always video-compatible conferences. If you wish to use MeetNow! conferences, the **Video** option must therefore be activated on at least one OpenScape Media Server.

---

### Numbering plan

Each OpenScape user is assigned to an individual office code via his/her ONS number. [Numbering plan](#) defines which office code an OpenScape user must be assigned to for the relevant OpenScape Media Server to provide a conference created by this user preferentially.

---

**NOTICE:** In case of MeetNow! conferences the creator is the OpenScape user who dials into the conference first. For all other conference types the creator is the OpenScape user who creates or initiates the relevant conference in his/her OpenScape client.

---

### Add

Adds the office code selected in the **Office Codes** field to the office code list.

### Remove

Removes the office codes the check boxes of which are enabled from the office code list.

## 15.4.3 Miscellaneous Number Settings

### MeetNow! Configuration

In the conference portal plugin, you can configure the following setting for MeetNow! conferences. This setting refers only to the default terminal **conferencing-MeetNow!** of all available OpenScape Media Servers.

Call-In number:

955

### Call-In number

Defines the phone number under which you can start MeetNow! conferences in the conference portal and conference participants need to dial into the conference portal.

### Direct PIN Call

*Default:* disabled

Conference notifications sent by e-mail may contain special links to facilitate joining a conference by mobile device. Using one of these links the conference participant accesses directly the associated conference room. He/she need not specify the conference's room number and access PIN manually. Such information is already contained in the respective link.

[Direct PIN Call](#) specifies whether e-mail notifications for conferences contain special links to facilitate dialing into a conference by mobile device.

---

**NOTICE:** If you wish to use this feature, the communications system used and the involved provider must be able to transmit long phone numbers without cutting them. The E.164 standard guarantees e. g. transmitting phone numbers up to 15 digits. Furthermore, routing of the communications system used must be configured to rout the relevant connections to the OpenScape Media Server.

---

---

**NOTICE:** For Screen Sharing to work when the Direct PIN Call feature is enabled, you should create a new address binding in the conferencing terminal. For this, open CMP and navigate to Media Server > Terminals > conference-default-addnumbers. In the Address field, add the extension of your conference bridge. By default, the conference bridge is 998.

---

### Moderator PIN

*Default:* disabled

In moderated conferences the participants are identified based on the phone number that was included in the conference invitation. In case moderators want to use another phone number to dial in to the moderated conference, they need to enter the moderator's pin in order to join the conference with moderator's permissions. Conference notifications to moderators sent by e-mail contain the moderator's pin and instructions about how to access the conference as a moderator.

---

**NOTICE:** You need to reboot OpenScape UC Application for the performed settings to take effect.

---

---

**NOTICE:** In case the Moderator PIN is activated, it is recommended to set **ModConfRequiresDialOutModerator** value to **false**. To do this follow the path: **CMP > Maintenance > Inventory > Nodes > [Application Node] > Show Services Status > Conferencing Service**.

---

The Moderator PIN can be set up to a certain length (default is 7), with minimum and maximum values, e.g. 0000000 to 9999999.

## 15.5 Media Configuration

In the conference portal, you can also configure the default language, as well as the audio, video, video performance and web settings.

### 15.5.1 Default language

*Default:* English (United States)

*Possible values:* <Languages for which the associated language RPMs have been installed>

After a user has logged in to the conference portal, the portal attempts to find the user in the OpenScape user database and to evaluate the user-individual voice settings. If the conference portal can determine a user language that supports the conference portal, the conference portal TUI is switched to the relevant language. If the determined user language is not available to the conference portal or the caller cannot be uniquely identified, the TUI is played in the language selected under [Default language](#).

The language selected here is also used for outbound calls of the conference portal if the conference portal cannot identify the caller as OpenScape user.

#### **Automatic cleanup of conferences after system user deletion**

*Default:* active

If this option is activated, the conference portal removes those participants from all scheduled conferences who do not exist any more as OpenScape users. Furthermore, all conferences the creator of which does no longer exist as OpenScape user are deleted.

#### **Dependent configuration overview**

Shows the status of configurations which need to be configured for other components to grant a smooth operation of the conference portal.

### 15.5.2 Audio Settings

#### **Sensitivity level**

As a rule, the image of the active speaker should react to a change of the person who conducts the conversation slightly delayed. This prevents the image of the active speaker from changing too often. [Sensitivity level](#) determines the duration of this delay. It can be set from very slow to super fast.

### 15.5.3 General - TUI Settings

In the conference portal plug-in you can configure the following settings for the conference portal TUI:

### Play neutral welcome instead of branded one

*Default:* active

The conference portal may use one of the following welcome announcements:

- Neutral, product-independent welcome announcement
- OpenScape welcome announcement

If the [Play neutral welcome instead of branded one](#) option is activated, the conference portal uses the neutral, product-independent welcome announcement. If the option is deactivated, the OpenScape welcome announcement is used

### Short greeting when entering conference room (less prompts)

*Default:* active

After conference participants have dialed into a conference and are connected to other participants, a welcome greeting can be played to them. If the [Short greeting when entering conference room \(less prompts\)](#) option is activated, the conference portal suppresses this welcome announcement.

---

**NOTICE:** This setting is relevant for audio but not for video devices.

---

### Fast transfer to conference room (no connecting prompts)

*Default:* active

The announcements of the conference portal are divided into two levels:

- Level 1: Announcements for essential information e. g. "Please enter your PIN"
- Level 2: Announcements for supplementing information e. g. "Your PIN has been accepted"

If the [Fast transfer to conference room \(no connecting prompts\)](#) option is activated, the conference portal suppresses the level 2 announcements.

### Play beep tone instead of longer join or left prompt (setting ignored when using name recording)

*Default:* active

The conference participants can be informed by announcements when another participant logs in to the conference or a logged in participant leaves the conference.

If the [Play beep tone instead of longer join or left prompt \(setting ignored when using name recording\)](#) option is activated, only a signal tone is played instead of the announcements.

---

**NOTICE:** Participant signaling is in moderated conferences only active by default as long as the number of dialed-in participants does not exceed 14. If, for example, the 15th participant dials in, the other conference participants will not be notified any more. Consequently, participants in very large conferences are not constantly disturbed by announcements / signal tones when new participants enter the room or present participants leave

---

it. [Changing the Participant Signaling Restriction](#) on page 475 describes how to change the setting that restricts participant signaling.

---

### Automatic Gain-Control - improved audio quality

*Default:* disabled

Defines whether different audio channel levels of a conference are automatically adjusted to each other. This adjustment reduces volume fluctuations between the single conference participants and those speaking in a softer voice can be heard as well.

### Number of joined participants determining suppression of join/leave indication

*Default:* 15

The conference participants can be informed by an announcement or signal tone when another participant joins the conference or a logged in participant leaves the conference. **Number of joined participants determining suppression of join/ leave indication** specifies from which number of conference participants participant signaling shall become inactive. Enter 11, for example, if participant signaling is to be active up to ten participants. Additionally, it specifies the number of participants for stopping the automatic refresh of the conference call control. After the threshold is reached, the automatic refresh stops. Users can click the refresh button that appears in the OpenScape Web Client in order to manually update the conference participants and their states.

This setting also limits the number of conference participants displayed in the conference control of the OpenScape clients. The following behavior applies:

- If the sum of dialed-in and invited but not dialed-in conference participants exceeds the value of [Number of joined participants determining suppression of join/leave indication](#), the conference control of the OpenScape clients only displays the dialed-in conference participants.
- If the number of dialed-in conference participants alone exceeds the value of [Number of joined participants determining suppression of join/leave indication](#), the conference control of the OpenScape clients displays the following only:
  - In an open conference: The local participant only.
  - In a moderated conference: The local participant and the dialed-in conference moderators. The number of displayed moderators is restricted to: [Number of joined participants determining suppression of join/leave indication](#) – 1

---

**NOTICE:** Which moderators are displayed in case of a restriction is determined randomly and may vary from client to client.

---

Even if the conference control of the OpenScape clients does not display all conference participants, the number of dialed-in conference participants is always indicated correctly.

## 15.5.4 Video Settings

In the conference portal plug-in, you can perform the following setting for representing Video conferences.

### Layout types

Determines in which manner the conference portal can represent the video images of the conference participants on the device displays of the participants. You can select the following options:

- Tile-based layout

The conference portal represents video images of the conference participants using video screens of the same size and as equal components. The number of video screens the device display is divided into depends on the number of participants in the conference. When the number of conference participants changes, the conference portal adjusts the number of video screens up to a specific maximum automatically. If this maximum is exceeded, the video images of the redundant participants are not displayed. When a represented participant leaves the conference for good, another participant not considered so far takes his/her place.

- Active speaker layout

The conference portal represents video images of the conference participants using video screens of the same size and as equal components. In addition, an enlarged video screen always shows the conference participant who is currently talking. The number of video screens the device display is divided into depends on the number of participants in the conference. When the number of conference participants changes, the conference portal adjusts the number of video screens up to a specific maximum automatically. If this maximum is exceeded, the video images of the redundant participants are not displayed. When a represented participant leaves the conference for good, another participant not considered so far takes his/her place.

- Active speaker only layout

The conference portal shows on the device display only the video image of the conference participant who is currently talking. As a rule, the image of this active speaker reacts to a change of the person who conducts the conversation slightly delayed. This prevents the image of the active speaker from changing too often.

After the conference start, each conference participant can switch to one of the selected layouts via the video menu. Depending on the setting performed for [Individual Views On](#), such a switch affects the representation for all conference participants or only for the conference participant who switches the layout.

### Default Layout

Specifies the layout every conference is started with. After the conference start, each conference participant can switch the layout via the video menu. In this case only layouts activated under [Layout types](#) are available. Depending on the setting performed for [Individual Views On](#), such a switch affects the representation for all conference participants or only for the conference participant who switches the layout.

### Individual Views On

With this option being active, the conference portal mixes an individual conference image for each conference participant. This enables conference participants to suppress their own image within the conference image by selecting the appropriate setting in the client. This also enables each conference participant to set his/her preferred layout.

## 15.5.5 Video Performance Settings

In the conference portal plug-in you can specify the resolution values for the available codecs. An example is resolution hd1080 or hd720 for the codecs h264 or h265. The resolution may vary from lowest to best.

## 15.6 Other Settings

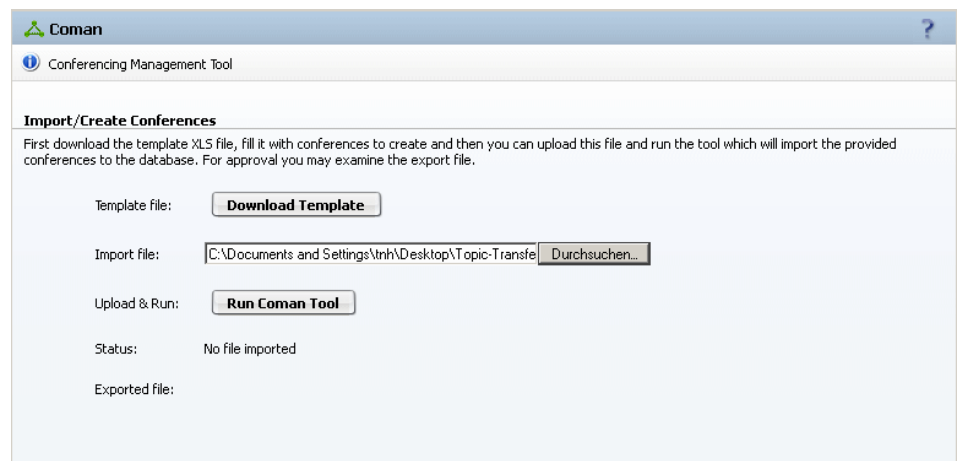
This section includes the following configuration settings:

- 1) The [Coman Tool](#) to configure conference management.
- 2) The [Recording](#) settings to configure the conference playback.
- 3) The [Notification Settings](#), to configure e-mail options.
- 4) The [Conference Viewer](#) to configure the URL for external participants.

### 15.6.1 Coman Tool

OpenScape UC Application is shipped with the conference management tool Coman. It provides features for managing the conferences of the conference portal independently of its clients:

These features are based on an import / export table in the format of Excel 97.



The screenshot shows the 'Coman' application window. The title bar says 'Coman' with a question mark icon. Below the title bar is a menu bar with 'Conferencing Management Tool'. The main area is titled 'Import/Create Conferences' and contains the following text: 'First download the template XLS file, fill it with conferences to create and then you can upload this file and run the tool which will import the provided conferences to the database. For approval you may examine the export file.' Below this text are four rows of controls: 1. 'Template file:' with a 'Download Template' button. 2. 'Import file:' with a text box containing 'C:\Documents and Settings\Unh\Desktop\Topic-Transfe' and a 'Durchsuchen...' button. 3. 'Upload & Run:' with a 'Run Coman Tool' button. 4. 'Status:' with the text 'No file imported'. At the bottom, there is an 'Exported file:' label.

#### Download Template

Loads an empty import / export table onto the computer system of the CMP used. You find details about the structure of the import / export table in [Import / Export Table for Bulk Processing](#) on page 775.

### **Import file**

Determines the file of an import / export table to be imported in OpenScape UC Application for managing conferences.

### **Run Coman Tool**

Imports the specified file of an import / export table in OpenScape UC Application and starts processing by the Coman tool.

### **Status**

Displays the current work status of the Coman tool.

### **Exported file**

Displays the name and storage location of a file that the Coman tool exports after finishing its processing. In this file the Coman tool documents the processing results.

## **15.6.2 Recording**

The OpenScape Unified Communications application provides a server sided conference recording, where all conference media can be recorded, stored in a central location, downloaded and managed.

Recorded media types include audio, video, web sharing and the 'Second Screen' supported by certain devices.

The server sided recording has to be differentiated from a client sided recording. The server sided recording does not require a special client. It can be initiated from any DTMF capable device. Only conference moderators have the privileges to start or stop a conference recording.

The recording is realized on the OpenScape Media Server node that hosts the respective conference. After the conference ends and the recording stops, the recorded file is automatically transferred to the recordings' data store that is the backend's directory: `/var/siemens/data/StorageService/conference`.

An e-mail with the download link to the recording and the expiration date is sent to the moderators. To enable the system to send this e-mail, a valid e-mail address must be stored in the moderator's UC profile. If no e-mail address is available, the recording will not be started. The recordings are stored for a limited time (configurable in CMP).

Note:

In case no recording licenses have been installed in the system (feature: OSC UC Appl Recording)

Navigate to:

`/opt/siemens/HiPathCA/config/common/WebClientUI.cfg`

In the WebClientUI.cfg file, set the value of the following parameter to false:

`allowConferenceRecording = false`

When it is false, the conference recording option on the Fusion hamburger menu and the WebClient will not appear.



If it is not set there is no functional impact as the option will be available but the recording will never start due to missing licenses.

### 15.6.2.1 Recording settings

The Recording settings section includes options for the actual configuration of the recording feature:

- The General section includes settings that apply to all kinds of conference recordings.
- The Video section includes settings that are specific for recordings of video conferences.

Recording settings - Internet Explorer

**Recording settings**

Settings for recording of audio and video conferences

**Recording settings** | **Recording list**

**General**

General settings

Disable voice notification on recording start ☐

Max. recording length (hours)

Notify the moderator that max. recording time is reached (minutes)

Recording expiration time (days)

Configure DTMF command for recording initiation: [DTMF Settings](#)

**Video**

Video settings

Disable flashing recording symbol (red dot) in video menu ☐

Resolution

Container format

Audio codecs

Recording video layout

Switch to second source when available ☒

Video Layout for second source

#### General

**Disable voice notification on recording start:** Disables the playback of a voice prompt, announcing that the conference is recorded, paused or resumed respectively. The default value is false, i.e. unchecked.

**Max. recording length:** Defines the maximum length of a single recording in hours. Note that only the recording will be stopped when this limit is exceeded, the actual conference can be continued. The default value is 5 hours.

**Notify the moderator that max. recording time is reached:** Before the maximum recording time is reached, a voice prompt is played to notify the user that the

recording is about to end. This value defines when this prompt will be played. The default value is 5 minutes.

Recording expiration time: Defines how long the recording will be available for download. After the time is expired, the conference will be deleted automatically from the conference server and will therefore not be available any more. The default value is 14 days.

Configure DTMF command for recording initiation: Opens the DTMF settings (see [DTMF settings](#) on page 740) in the Conference configuration dialog. In this section, you can configure the DTMF key(s) to start/pause the conference recording. The key to start, pause and resume the recording is the same for all three actions. The default value is \*7. Thus, a conference recording starts when DTMF '\*7' is detected. A second '\*7' pauses the recording, a third '\*7' resumes it. The recording is actually stopped when the conference ends. Alternatively, the latest version of the FastViewer client can be used to control the recording.

### Video

Disable flashing recording symbol in video menu: When this option is unchecked, a 'recording' icon (red dot) is displayed on the top right corner of the video window indicating that a recording is active. When this option is checked, no icon is displayed. The default value is off, i.e. unchecked.

Resolution: Defines the video resolution. Options are VGA, HD or Full HD.

Container format: Defines the container format of the resulting video. The default value is MP4.

---

**NOTICE:** Note that the container format is selected here, not the actual audio or video codec. Currently, video uses always the H.264 codec. When MP4 is selected, MP3-audio is used as audio codec, while PCM audio is used for Matroska.

---

Audio codecs: This option is currently informational. No codecs can be selected.

Recording video layout: Defines the video layout for the recording. All active video layouts, as defined in the Video settings section (see [Video Settings](#) on page 754) can be selected here.

Switch to second source when available: When the checkbox is checked, the recording will also record a 'second source' video when it becomes available. The default value is on, i.e. checked.

Video layout for second source: Defines the video layout when a conference with an additional second source is recorded, currently available values:

- Presentation Active Speaker: the presentation takes most of the place on the screen, but the video participants are also visible in smaller tiles.
- Presentation only: only the presentation can be seen in the recording.

The default value is Presentation Active Speaker.

## 15.6.2.2 Recording list

The Recording list displays a searchable list of the recordings currently stored and their status.

## Conference Portal Settings in the CMP (Conference Portal Plug-in)

**Recording settings**

Settings for recording of audio and video conferences

**Recording settings** | **Recording list**

**Recording list**

To search for recordings please enter some term and push the update button

Search term:

Orphaned: ☐

**Update list**

**Delete...**

Self: 0 | Items/Page: 50 | All: 31

|                          | Title                   | Date                | Duration | Media | Size    | Expiration Time | Status        |
|--------------------------|-------------------------|---------------------|----------|-------|---------|-----------------|---------------|
| <input type="checkbox"/> | RecordingTestAudioVideo | 5/12/15 4:49:28 PM  | 31 sec.  |       | 1179 KB | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioVideo | 5/12/15 3:46:58 PM  | 20 sec.  |       | 2436 KB | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioVideo | 5/12/15 3:42:42 PM  | 13 sec.  |       | 1834 KB | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioVideo | 5/12/15 3:33:09 PM  | 15 sec.  |       | 2701 KB | Expired         | Transfer done |
| <input type="checkbox"/> | TestFV1                 | 5/12/15 3:16:37 PM  | 94 sec.  |       | 7 MB    | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 3:10:37 PM  | 23 sec.  |       | 1204 KB | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 3:07:34 PM  | 28 sec.  |       | 887 KB  | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 3:03:43 PM  | 25 sec.  |       | 395 KB  | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 3:03:07 PM  | ---      |       | ---     | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 2:48:41 PM  | 17 sec.  |       | 263 KB  | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 2:44:58 PM  | 15 sec.  |       | 239 KB  | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 2:44:30 PM  | ---      |       | ---     | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 2:38:54 PM  | 14 sec.  |       | 679 KB  | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 12:47:47 PM | 17 sec.  |       | 1063 KB | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 12:37:50 PM | 20 sec.  |       | 5 MB    | Expired         | Transfer done |
| <input type="checkbox"/> | RecordingTestAudioOnly  | 5/12/15 12:27:51 PM | 19 sec.  |       | 6 MB    | Expired         | Transfer done |

**Save** **Cancel**

### Search options

**Search term:** The complete recordings list is shown. You can enter a search phrase to retrieve a specific recording title. All conference recordings with a matching title will be displayed after clicking Update list.

**Orphaned:** Orphaned conference recordings are still stored while the respective conference has already been deleted. To search for all orphaned recordings, select the checkbox and click Update list. The default value is off, i.e. unchecked).

### List of Conference Recordings

**Title:** The title of the recorded conference.

**Date:** Date and time of the recording.

**Duration:** Duration of the recording (not of the respective conference). The duration is displayed after conference completion. If the recording is currently in progress, the duration is not displayed.

**Media:** The recorded media types, such as audio, video and web sharing.

## Conference Portal Settings in the CMP (Conference Portal Plug-in)

**Size:** File size of the recording. This is displayed after the conference ends. When the recording is currently in progress, the size is not shown.

**Expiration Time:** Timespan until the recording expires and will be removed from the data store. When a recording is expired, it is not available for download any more.

**Status:** Current status of the recording. Possible values:

- --- (unknown): The conference is currently in progress
- Transferring: The recording was just stopped and the file is currently transferred to the data store
- Transfer done: The recording has been successfully stored on the data store and can be downloaded from there

You can also delete one or more recordings from the list. Select the recording to be deleted and click Delete to permanently remove the recording from the data store.

You can also download one or more recordings from the list. Select the recording to be downloaded and click Download to download and/or playback the recording.

---

**NOTICE:** Up to four video sending parties should be shown directly in the active speaker recording layout (which is 1 large content + 4 small tiles on the right). With more than 5 sending parties the active speaker tile should be on top right and the remaining is filled in the order of entering /starting video sending. For filling the small tiles below the active speaker the moderators should have preference over users so that there is a sort of small discussion panel of moderators which is always visible in the video. - Grace periods (greyed out tile) in case of temporary disconnect - Grace period (greyed out tile) in case of a person is no longer sending a video (if applicable) - Showing one person in both his / her tile and the active speaker tile to avoid rearrangements

---

### 15.6.3 Notification Settings

The conference portal sends e-mail notifications to conference participants on different occasions. The texts of such notifications are pre-configured for all conference portal TUI languages and thus available after the conference portal has been installed.

Before the conference portal sends the e-mail notification to a conference participant, it attempts to identify the participant as OpenScape user. In this process it searches the OpenScape user database for the relevant conference participant.

If the conference portal manages to identify the conference participant in this way, it determines the user-individual language setting from the user settings and sends the e-mail notification in this language then. This requires the text of the e-mail notification being available in the language thus determined.

If the text of the e-mail notification is unavailable in the determined language or the web conference participant cannot be found in the OpenScape user database, the system sends the e-mail notification in English (US).

## Conference Portal Settings in the CMP (Conference Portal Plug-in)

In the conference portal plug-in you can perform the following setting for e-mail notifications of the conference portal:

**Notification settings** ?

Participant notification settings

**E-mail notification**  
E-mail notifications for conference users

Send e-mail: ☒

**E-mail notification (content)**  
List of language dependent e-mail notifications

Items/Page: 10 | All: 10

| Short name | Name                     |
|------------|--------------------------|
| en_gb      | English (United Kingdom) |
| en_us      | English (United States)  |
| pt_br      | Portuguese (Brazil)      |
| zh_cn      | Chinese (China)          |
| ru_ru      | Russian (Russia)         |
| pt_pt      | Portuguese (Portugal)    |
| de_de      | German (Germany)         |
| es_es      | Spanish (Spain)          |
| it_it      | Italian (Italy)          |
| fr_fr      | French (France)          |

**Conference viewer**  
Conference viewer settings for external participants

URL Configuration:

### Send e-mail

Specifies whether the conference portal may send automatically generated e-mail notifications. If the [Send e-mail](#) option is active, the conference portal sends e-mail notifications to participants whose e-mail addresses are known in the OpenScape system on fixed occasions. See also [Trigger name](#).

### <list of supported notifications>

Indicates the languages in which the conference portal can send automatically generated e-mail notifications. By default, languages are displayed for which the associated language RPM has been installed. To select the relevant entry, enable the radio button that precedes the respective list entry. You can then remove the selected entry from the list. See [Remove](#). You can use the [Edit \(in the Action menu\)](#) option of a list entry to edit the notification text of the relevant language.

### Edit (in the Action menu)

Opens a configuration dialog in which you can edit the notification text of the relevant language.

### Remove

Removes the selected entry from the list.

---

**NOTICE:** You cannot remove notification languages available in the list by default.

---

### Add

Opens a configuration dialog to add an additional language to the list of supported notification languages.

### URL Configuration

Specifies the URL under which conference participants of another UC Application cluster can access the restricted conference connection control. For Very Large Deployment you need to specify the URL under which the OpenScape Web Client of the local UC Application cluster can be reached.

---

**NOTICE:** Configure this setting for Very Large Deployment only.

---

You can edit the e-mail notification text specific to a language. In the conference portal plug-in, you can configure the following setting for this purpose:

**E-mail notifications** ?

ⓘ Edit subject and body parts of the e-mail notification which will be send to the users cause of some conferencing event (trigger).

E-mail notification for language: **English (United Kingdom)**

Trigger name:

Subject:

Included body parts: **Invitation** General Audio Video Web Viewer

You are invited to conference %subject%

Placeholders:   Conference creator

### E-mail notification for language

Indicates the language for which the notification text is being edited.

### Trigger name

The contents of the notification text depends on the event for which the conference portal sends the notification. [Trigger name](#) indicates the event for which the notification text is edited.

The following triggers can be selected:

## Conference Portal Settings in the CMP (Conference Portal Plug-in)

- |                                                                                                                                                                                   |                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• <b>Conference created</b></li> <li>• <b>Conference updated</b></li> <li>• <b>PIN regenerated</b></li> <li>• <b>User added</b></li> </ul> | <ul style="list-style-type: none"> <li>• <b>User deleted</b></li> <li>• <b>Web added</b></li> <li>• <b>Audio added</b></li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

### Subject

Defines the subject line of the e-mail notification that the conference portal sends in the event of the selected trigger. You can paste the entry under [Subject](#) also in the actual notification text via a corresponding wildcard (cf. [Placeholders](#)).

### Included body parts

The body of the notification text consists of various parts. Under [Included body parts](#) the body parts contained in the notification text for the selected trigger are listed. A click on the displayed name shows the associated notification text in the text field where it can be edited.

Depending on the selected trigger, the notification text contains the following selectable body parts:

| Body part           | Available for trigger |                    |                 |            |              |           |             |
|---------------------|-----------------------|--------------------|-----------------|------------|--------------|-----------|-------------|
|                     | Conference created    | Conference updated | PIN regenerated | User added | User deleted | Web added | Audio added |
| • <b>Invitation</b> | ✓                     |                    |                 | ✓          |              |           |             |
| • <b>General</b>    | ✓                     | ✓                  | ✓               | ✓          |              |           | ✓           |
| • <b>Audio</b>      | ✓                     | ✓                  | ✓               | ✓          |              |           | ✓           |
| • <b>Video</b>      | ✓                     | ✓                  | ✓               | ✓          |              |           | ✓           |
| • <b>Web</b>        | ✓                     | ✓                  | ✓               | ✓          |              | ✓         |             |
| • <b>Viewer</b>     | ✓                     | ✓                  | ✓               | ✓          |              |           | ✓           |

### Placeholders

Variable information may have to be pasted in the notification text – e. g. the name of the respective conference creator. To do this, various wildcards are available, which you can position in the notification text. Under [Placeholders](#) you can select the wildcard to be pasted in the notification text where the cursor is currently positioned.

---

**NOTICE:** You cannot paste any wildcards in the **Subject** field.

---

The following wildcards can be selected:

|                                             |                                                                                                                                                                                |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • <b>Subject</b>                            | Pastes the text from the <a href="#">Subject</a> setting.                                                                                                                      |
| • <b>Toll number</b>                        | Pastes the general access number under which participants can dial into the conference. This access number is determined under Toll number.                                    |
| • <b>Toll number (easy join)</b>            | Pastes the easy join access number under which participants can dial into the conference. This access number is determined under Toll number (easy join).                      |
| • <b>Toll number (easy join, moderator)</b> | Pastes the easy join access number under which moderators can dial into the conference. This access number is determined under Toll number (easy join, moderator).             |
| • <b>Toll number (OSMO)</b>                 | Pastes the OSMO access number under which participants can dial into the conference. This access number is determined under Toll number (OSMO).                                |
| • <b>Toll number (OSMO, moderator)</b>      | Pastes the OSMO access number under which moderators can dial into the conference. This access number is determined under Toll number (OSMO, moderator).                       |
| • <b>Additional number</b>                  | Pastes additional access numbers under which participants can dial into the conference, such as Toll free numbers. Such access numbers are determined under Additional number. |
| • <b>Creator</b>                            | Pastes the conference creator.                                                                                                                                                 |
| • <b>Start time</b>                         | Pastes the conference start time.                                                                                                                                              |
| • <b>PIN</b>                                | Pastes the PIN for entering the conference.                                                                                                                                    |
| • <b>Moderator PIN</b>                      | Pastes the moderator PIN for entering the conference.                                                                                                                          |
| • <b>WEB Provider</b>                       | Pastes the name of the conference system used for the conference.                                                                                                              |
| • <b>Web-Participant URL</b>                | Pastes the URL under which external conference participants can download the Web Conference application for taking part in a Web conference.                                   |
| • <b>Web Client URL</b>                     | Pastes the URL under which external conference participants can take part in a Web Conference without having to download the Web Conference application.                       |



|                                       |                                                                                                                                                                                                                |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • Viewer URL                          | Pastes the URL under which conference participants of another UC Application cluster can access the restricted conference connection control. This URL is determined under <a href="#">URL Configuration</a> . |
| • Recording URL                       | Pastes the URL under which conference participants can view/download the conference recording. By default, the URL created is based on the BE node hostname.                                                   |
| • Recording size                      | Pastes the recording size.                                                                                                                                                                                     |
| • Expiration time                     | Pastes the expiration time.                                                                                                                                                                                    |
| • DTMF code for “Enter moderator PIN” | Pastes the DTMF code for entering the moderator PIN.                                                                                                                                                           |

### insert

- 1) Pastes the wildcard selected under [Placeholders](#) in the notification text where the cursor is currently positioned.

### Show preview / back to Editor

Two views of the text field are available for editing the notification text.

- The editor view in which only the respectively selected body part is displayed and can be edited for the selected trigger.
- The preview that always displays the entire notification text for the selected trigger. Neither the displayed text nor the display options can be edited in this view.

Using [Show preview / back to Editor](#) you can toggle the two views.

## 15.6.4 Conference Viewer

The URL configuration of the Conference Viewer for external participants.

User can see the members of the conferences and the PIN, but there is no call control on the conference before clicking on “Login”. In order to have call control, user has to click on “Login” manually.

## 15.6.5 Add join conference beep

Starting with V11R6, the join conference beep has been removed. However, users can still hear the beep sound by configuring the `playJoinLeftPrompt` setting according to the instructions below:

- 1) Navigate to the following path:  
`/opt/siemens/mediaserver/application_host/  
deployment/conferencingapplets/  
ConferencingApplication.application.xml`
- 2) Set the `playJoinLeftPrompt` parameter to `true`.

## 16 General Properties for the Conference Portal

To start the conference portal with an individual configuration you can configure the corresponding general properties in the associated Media Server terminal. The OpenScape Media Server then transfers these general properties when you invoke the conference portal.

---

**NOTICE:** You can configure the most important conference portal settings also via the graphic configuration interface of the conference portal – via the conference portal plug-in.

---

The conference portal supports the following general properties.

- [calloutGracePeriod](#)
- [displayName](#)
- [dtmfConfig](#)
- [dtmfKeyDelay](#)
- [fastTransfer](#)
- [fastWelcome](#)
- [language](#)
- [rejoinGracePeriod](#)
- [maximalParticipants](#)
- [neutralWelcome](#)

### **calloutGracePeriod**

*Default:* 30 000 [ms]

*Possible values:* <Time> [ms]

*Example:*

- **Key–** [calloutGracePeriod](#)
- **Value–** 30000

You find a description of this setting in [Timer settings](#) on page 743 under [Call-out ring timeout](#).

### **displayName**

*Default:* Conference Bridge

*Possible values:* <text>

*Example:*

- **Key–** [displayName](#)
- **Value–** Conference portal

### **dtmfConfig**

You need to configure this setting via the conference portal plug-in. You find a description on this in [DTMF settings](#) on page 740.

### **dtmfKeyDelay**

*Default:* 30 000 [ms]

*Possible values:* <Time> [ms]

*Example:*

- **Key**– [dtmfKeyDelay](#)
- **Value**– 30000

Conference participants can control selected functions of the conference portal DTMF-based. Two successive key entries result in one control command.

[dtmfKeyDelay](#) defines the interval in which a user needs to press two keys for them to be interpreted as a coherent control command.

### **fastTransfer**

*Default:* true

*Possible values:*

- true – Level 2 announcements are played
- false – Level 2 announcements are not played.

*Example:*

- **Key**– [fastTransfer](#)
- **Value**– true

You find a description of this setting in [Timer settings](#) on page 743 under [Fast transfer to conference room \(no connecting prompts\)](#).

### **fastWelcome**

*Default:* true

*Possible values:*

- true – Do not play welcome greeting
- false – Play welcome greeting.

*Example:*

- **Key**– [fastWelcome](#)
- **Value**– true

You find a description of this setting in [Timer settings](#) on page 743 under [Short greeting when entering conference room \(less prompts\)](#).

### **language**

*Default:* en\_us

*Possible values:*

- de\_de – German (Germany)
- en\_gb – English (UK)
- en\_us – English (USA)
- es\_es – Spanish (Spain)
- fr\_fr – French (France)
- it\_it – Italian (Italy)
- pt\_br – Portuguese (Brazil)
- pt\_pt – Portuguese (Portugal)
- zh\_cn – Chinese (Mandarin)

*Example:*

- **Key**– [language](#)
- **Value**– en\_us

You find a description of this setting in [Media Configuration](#) on page 751 under [Default language](#).

### **rejoinGracePeriod**

*Default:* 300 000 [ms]

*Possible values:* <Time> [ms]

*Example:*

- **Key**– [rejoinGracePeriod](#)
- **Value**– 300000

You find a description of this setting in [Timer settings](#) on page 743 under [Rejoin grace period](#).

### **maximalParticipants**

*Default:* 200

*Possible values:*

- <positive number>
- -1 – Unlimited number of conference participants

*Example:*

- **Key**– [maximalParticipants](#)
- **Value**– 10

Defines the maximum number of participants who may take part in every conference.

### **neutralWelcome**

*Default:* true

*Possible values:*

- true – neutral welcome announcement
- false OpenScape-welcome announcement.

*Example:*

- **Key**– [neutralWelcome](#)
- **Value**– true

You find a description of this setting in [Timer settings](#) on page 743 under [Play neutral welcome instead of branded one](#).

## 17 Managing the Conference Video Layout

This chapter provides information about the following topics of the video layout management:

- [Concept of Managing Video Layouts](#)
- [Structure of the resolution.xml file](#)
- [Structure of the Files screen-layout-....xml](#)

### 17.1 Concept of Managing Video Layouts

The conference portal represents the video streams of a video conference in a video layout, which is optimized for the respectively playing device. Various video layouts are pre-configured for the conference portal by default, so that it can already cooperate with many video devices after the setup.

Video layouts are defined using the following configuration files and can be modified or supplemented using these files:

- `resolutions.xml`

Defines the video resolutions that the conference portal can use for the possible video layouts. As a rule, you need not make any individual adjustments in this file.

- `level-resolution.xml`

Defines the video resolution that the conference portal uses if it has negotiated a specific H.264 profile level ID for a connection with the video device. Because you need not make any individual adjustments in this file, the following descriptions do not consider it in detail.

---

**NOTICE:** You find a description of the standardized H.264 profile level IDs e.g. under the following link:

[http://en.wikipedia.org/wiki/H.264/MPEG-4\\_AVC#Levels](http://en.wikipedia.org/wiki/H.264/MPEG-4_AVC#Levels)

---

- `screen-layout-....xml`

These files define the structure of the various video layout types. In these files you can customize available video layouts and define additional ones.

All described configuration files are stored after the OpenScape UC Application setup in the following directory of the application computer:

`<Osc-Install101>/mediaserver/application_host/bin/res/layout`

---

**IMPORTANT:** Always back up the configuration files before modifying them.

---

---

<sup>101</sup> `<Osc-Install>` is the setup directory of OpenScape UC Application: `/opt/siemens/` respectively `/enterprise/`

## 17.2 Structure of the resolution.xml file

The configuration file `resolution.xml` specifies the video resolutions that can be used for the possible video layouts.

```
<Resolutions>
 <!-- 16:9 (+3x2) -->
 <Resolution Label="hd1080" Width="1920" Height="1080" />
 <Resolution Label="1536x864" Width="1536" Height="864" />
 <Resolution Label="1440x810" Width="1440" Height="810" />
 <Resolution Label="hd720" Width="1280" Height="720" />
 <Resolution Label="1024x576" Width="1024" Height="576" />
 <Resolution Label="960x768" Width="960" Height="768" />
 <Resolution Label="960x540" Width="960" Height="540" />
 <Resolution Label="960x360" Width="960" Height="360" />
 <Resolution Label="854x480" Width="854" Height="480" />
 <Resolution Label="640x540" Width="640" Height="540" />
 <Resolution Label="640x360" Width="640" Height="360" />
 <Resolution Label="640x240" Width="640" Height="240" />
 <Resolution Label="480x270" Width="480" Height="270" />
 <Resolution Label="426x360" Width="426" Height="360" />
 <Resolution Label="426x240" Width="426" Height="240" />
 <Resolution Label="384x216" Width="384" Height="216" />
 <Resolution Label="320x256" Width="320" Height="256" />
 <Resolution Label="320x180" Width="320" Height="180" />
 <Resolution Label="256x144" Width="256" Height="144" />
 ...
</Resolutions>
```

Each of the listed resolutions defines:

- A label used for referencing the video resolution in a video layout definition.
- The actual format of the video resolution in **Width** and **Height**.

To change existing video resolutions you simply need to adjust the associated format specifications.

To configure a new video resolution you need to add a new **Resolution** entry to the specified resolutions. In doing so you need to assign it a unique identifier under **Label** and define the desired format via **Width** and **Height**.

## 17.3 Structure of the Files screen-layout- . . . .xml

Depending on the device resolution and the number of conference participants, the configuration files `screen-layout- . . . .xml` define

- In which resolution the individual representations of the conference participants are displayed on the device screen.
- How the individual representations of the conference participants are grouped on the screen.
- The order in which the screen of the device is filled with the individual representations of the conference participants.

This is the complete list of configuration files each of which is assigned to an individual layout type.

- `screen-layout-accentuated-n+1.xml`  
This configuration file is used to control the video representation when the **Active Speaker** layout type is selected.
- `screen-layout-tiled.xml`  
This configuration file is used to control the video representation when the tile-based layout type is selected.
- `screen-layout-single.xml`  
This configuration file is used to control the video representation when the **Single** layout type is selected.

Depending on the layout type, the configuration files provide different configuration options. These configuration options are described in detail in the following sections.

### 17.3.1 Structure of the Files `screen-layout-accentuated-n+1.xml`

This configuration file is used to control the video representation when the **Active Speaker** layout type is selected.

```
<Screens>
 <Screen Resolution="hd720">
 <Layout Name="hd720(1)">
 <Tile Resolution="hd720" PosX="center" PosY="center"
label="ActiveSpeaker" />
 </Layout>
 <Layout Name="hd720(5+1)">
 <Tile Resolution="854x480" PosX="left" PosY="top"
label="ActiveSpeaker" />
 <Tile Resolution="426x240" PosX="right" PosY="top"
Label="#1" />
 <Tile Resolution="426x240" PosX="right" PosY="center"
Label="#2" />
 <Tile Resolution="426x240" PosX="right" PosY="bottom"
Label="#3" />
 <Tile Resolution="426x240" PosX="center" PosY="bottom"
Label="#4" />
 <Tile Resolution="426x240" PosX="left" PosY="bottom"
Label="#5" />
 </Layout>

 <Layout Name="hd720(7+1)">
 <Tile Resolution="960x540" PosX="left" PosY="top"
label="ActiveSpeaker" />
 <Tile Resolution="320x180" PosX="right" PosY="top"
Label="#1" />
 <Tile Resolution="320x180" PosX="right" PosY="180"
Label="#2" />
 <Tile Resolution="320x180" PosX="right" PosY="360"
Label="#3" />
 <Tile Resolution="320x180" PosX="right" PosY="bottom"
Label="#4" />
 <Tile Resolution="320x180" PosX="640" PosY="bottom"
Label="#5" />
 </Layout>
 </Screen>
</Screens>
```

```
<Tile Resolution="320x180" PosX="320" PosY="bottom"
Label="#6" />
<Tile Resolution="320x180" PosX="left" PosY="bottom"
Label="#7" />
</Layout>
...
</Screen>
...
</Screens>
```

The above extract shows possible layout settings for the device resolution with the name **hd720** (<Screen Resolution="hd720">. A device would be sent a video stream in one of these resolutions if the conference portal and the device had negotiated this resolution during the connection setup.

---

**NOTICE:** The following file defines the possible device resolutions with their corresponding names: `resolution.xml`

---

Several video layouts (Layout) are defined for the resolution with the name **hd720**. Each of these video layouts has been optimized for an individual number of conference participants. This number of conference participants is determined by the number of **Tile** entries a video layout contains.

---

**NOTICE:** The layout name (e. g. **hd720(5+1)**) does not technically refer to the number of participants and / or Video resolution. This text is freely selectable and used as reference in log outputs, for example.

---

Every **Tile** entry represents the image of a conference participant. The **Tile** entry with the **Label Active Speaker** defines the image of the conference participant who is currently speaking. The **Tile** entries with **#-Label** define the images assigned to participants of conference participants who have joined the conference.

^For example, the video layout with the name **hd720(5+1)** defines a **Tile** entry for the active speaker and five **Tile** entries for the representations assigned to participants of conference participants. As in this kind of layout, the active speaker is represented as active speaker and also as image assigned to a participant, this video layout is ideal for a video conference with five conference participants. Every single **Tile** entry defines the video resolution in which the relevant participant image is displayed (**Resolution**) and where this image is positioned on the device display (**PosX, PosY**). The number for each **#-Label** determines the order in which video streams are allocated to the images assigned to participants.

*Example:* A video conference participant A takes part in a video conference with his/her device. The conference portal has negotiated the video resolution hd720 with the device of A during the connection setup. Currently, there are a total of five participants in the conference.

Under these circumstances, the conference portal determines the video layout for the device of A from the following layout configuration. This choice is based on the fact that this layout has been optimized for five conference participants.

```
<Screens>
 <Screen Resolution="hd720">
```



```

...
<Layout Name="nhd(5+1)">
 <Tile Resolution="854x480" PosX="left" PosY="top"
label="ActiveSpeaker" />
 <Tile Resolution="426x240" PosX="right" PosY="top"
Label="#1" />
 <Tile Resolution="426x240" PosX="right"
PosY="center" Label="#2" />
 <Tile Resolution="426x240" PosX="right"
PosY="bottom" Label="#3" />
 <Tile Resolution="426x240" PosX="center"
PosY="bottom" Label="#4" />
 <Tile Resolution="426x240" PosX="left"
PosY="bottom" Label="#5" />
</Layout>
...
</Screens>

```

Within this layout, the image of the active speaker is displayed in the resolution with the name **854 x 480**. The images assigned to participants are represented in the resolution with the name **426 x 240**.

---

**NOTICE:** The following file defines the possible device resolutions with their corresponding names: `resolution.xml`

---

All images are arranged on the device screen according to the corresponding PosX/PosY specifications. The images assigned to participants are filled with video streams in the order of the **#-Label** numbering.

---

**NOTICE:** You find a description of all possible position specifications in the configuration file `screen - layout.xml`.

---

If a sixth conference participant dials into the conference, the layout with the name **nhd(5+1)** is not ideal any more for the number of conference participants. As a further layout has been defined for the same device resolution and more than five conference participants, the conference portal starts sending the video stream to the device of conference participant A in this layout.

```

<Screens>
 <Screen Resolution="hd720">
 ...
 <Layout Name="hd720(7+1)">
 <Tile Resolution="960x540" PosX="left" PosY="top"
label="ActiveSpeaker" />
 <Tile Resolution="320x180" PosX="right" PosY="top"
Label="#1" />
 <Tile Resolution="320x180" PosX="right" PosY="180"
Label="#2" />
 <Tile Resolution="320x180" PosX="right" PosY="360"
Label="#3" />
 <Tile Resolution="320x180" PosX="right"
PosY="bottom" Label="#4" />
 </Layout>
 </Screen>
</Screens>

```

```
<Tile Resolution="320x180" PosX="640" PosY="bottom"
Label="#5" />
<Tile Resolution="320x180" PosX="320" PosY="bottom"
Label="#6" />
<Tile Resolution="320x180" PosX="left"
PosY="bottom" Label="#7" />
</Layout>
...
</Screen>
...
</Screens>
```

Within this layout, the image of the active speaker is displayed in the resolution with the name **960 x 540**. The images assigned to participants are represented in the resolution with the name **320 x 180**.

If more than seven conference participants join in, the conference portal keeps the video layout, because no layout has been defined by default for more than seven participants. In this case, the images assigned to participants display only the first seven conference participants who joined in. All other conference participants are only temporarily displayed in the image of the currently active speaker – namely when the conference portal recognizes them as active speaker.

---

**NOTICE:** If no video layout that can represent all conference participants exists for a device resolution, the conference portal uses the layout that can represent the largest number of participants for the relevant device resolution. In this case you cannot individually control which conference participants are and are not displayed on a device. This behavior is controlled within the conference portal.

---

### 17.3.2 Structure of the Files `screen-layout-tiled.xml`

This configuration file is used to control the video representation when the tile-based layout type is selected.

Its structure is very similar to the one of the configuration file for the **Active Speaker** layout type (`screen-layout-accentuated-n+1.xml`) and can be adapted in the same way.

The only difference: The configuration file `screen-layout-tiled.xml` does not support **Tile** entries with the **Label Active Speaker**.

### 17.3.3 Structure of the Files `screen-layout-single.xml`

This configuration file is used to control the video representation when the **Single** layout type is selected.

Its structure is very similar to the one of the configuration file for the **Active Speaker** layout type (`screen-layout-accentuated-n+1.xml`) and can be adapted in the same way.

The only difference: The configuration file `screen-layout-single.xml` supports exclusively **Tile** entries with the **Label Active Speaker**.

## 18 Conference Management Tool Coman

This chapter provides information about the following topics of the Coman tool:

- [Coman Tool Function](#)
- [Import / Export Table for Bulk Processing](#)
- [Processing Conference Scheduling Specifications](#)
- [Logging the Coman Tool for Troubleshooting](#)
- [Installing the Coman Tool](#)
- [Invoking the Coman Tool](#)
- [Invoking the Online Help of the Coman Tool](#)
- [Command Reference for the Coman Tool](#)

### 18.1 Coman Tool Function

OpenScape UC Application is shipped with the conference management tool Coman. This tool operates based on Windows or Linux. It provides in particular the following features for managing the conferences of the conference portal independently of OpenScape UC Application and its clients:

- Bulk processing of conferences
- Creating conferences on the behalf of any existing OpenScape user.
- Creating one-off conferences and conference series.
- Creating PINs for audio conferences.
- Activating / deactivating video for conferences.
- Conference output according to definable.

### 18.2 Import / Export Table for Bulk Processing

The Coman tool supports bulk processing of conferences. This feature is based on an import / export table in the format of Excel 97.

Every row of an import / export table describes the data of an individual conference.

To display a help text for a table column in English language, click on ▼ in the header of the relevant column.

|   | A         | B     | C   | D     | E     | F        | G          | H            | I                                                              | J | K | L | M     | N             |
|---|-----------|-------|-----|-------|-------|----------|------------|--------------|----------------------------------------------------------------|---|---|---|-------|---------------|
| 1 | CreatorId | Audio | Web | Video | Title | AudioPIN | Moderators | Participants | Participants in the conference (comma seperated list of users) |   |   |   | Until | Conference ID |
| 2 |           |       |     |       |       |          |            |              |                                                                |   |   |   |       |               |

The import / export table contains the following columns for defining conference settings.

- **CreatorId**  
Defines the ID of the user account deployed as creator for the relevant conference.  
*Example:* mBrown@system

- **Audio**

Defines whether the relevant conference contains an audio stream. Possible values are:

- 0 – The conference does not contain an audio stream.
- 1 – The conference contains an audio stream.

- **Web**

Defines whether the relevant conference contains a web conference. Possible values are:

- 0 – The conference does not contain a web conference.
- 1 – The conference contains a web conference.

- **Audio**

Defines whether the relevant conference contains a video stream. Possible values are:

- 0 – The conference does not contain a video stream.
- 1 – The conference contains a video stream.

- **Title**

Defines the title of the relevant conference.

*Example:* Sales Department Meeting

- **AudioPIN**

Defines the audio PIN of the relevant conference.

*Example:* 5487

- **Moderators**

Defines the IDs of the user accounts deployed as moderators for the relevant conference. Several user accounts are separated by comma.

*Example:* mBrown@system, pWhite@system

- **Participants**

Defines the IDs of the user accounts deployed as participants for the relevant conference. Several user accounts are separated by comma.

*Example:* mBrown@system, pWhite@system

- **StartDate**

Defines the start time of the relevant conference. In this column, times must be specified continuously in one of the following formats:

- d.M.yy HH:mm (DE format)
- M/d/yy HH:mm (US format)

*Example (US format):* 4/18/11 14:32

If the table is imported in OpenScape UC Application and the US format is used, you need to specify this in the **dateFormat** parameter of the **importXLS** action.

- **Duration**

Defines the scheduled duration of the relevant conference. In this field you need to specify times in minutes.

- **StartDate**

Defines the repeat frequency of the relevant conference. Possible units for specified values are:

- Hourly / H – A conference is repeated every x hours.
- Daily / D – A conference is repeated every x days.
- Weekly / W – A conference is repeated every x weeks.
- Monthly / M – A conference is repeated every x months.
- Yearly / Y – A conference is repeated every x years.

If you specify a number without unit, the Coman tool uses the unit days (D).

*Example:* 4 W or 4 Weekly

- **Recurrences**

Defines the number of repeats after which the relevant conference series ends.

- **Until**

Defines the time until which the relevant conference series goes on. In this column you may have to specify times in the format also used in the **StartDate** column.

If the table is imported in OpenScape UC Application and the US format is used, you need to specify this in the **dateFormat** parameter of the **importXLS** action.

---

**NOTICE:** A time specification in this field is ignored if a value has also been entered under **Recurrences**.

---

- **ConferenceID**

Defines for the relevant conference an ID used within the system.

---

**IMPORTANT:**

You must not modify the values in this column.

---

## 18.3 Processing Conference Scheduling Specifications

You can make specifications in the following columns of the import / export table for scheduling a conference:

- **StartDate**
- **Duration**
- **Frequency**
- **Recurrences**
- **Until**

For specifications in these columns the following defaults apply:

**One-off ad-hoc conference**

For a one-off ad-hoc conference you need to enter a value in the **Duration** column. The resulting ad-hoc conference starts two minutes after the table was imported in OpenScape UC Application and lasts for the specified time.

### **One-off scheduled conference**

For a one-off scheduled conference you need to enter a value in the **StartDate** column. This generates a scheduled conference that starts at the specified time and lasts for 30 minutes.

If you wish the conference duration to differ from the default, specify the desired duration in the **Duration** column.

### **Conference series**

For a conference series you need to enter a value in one of the following columns:

- **Frequency**
- **Recurrences**
- **Until**

This creates a conference series for which the following applies:

- Each conference of the conference series lasts for 30 minutes.
- This first conference begins two minutes after the table was imported in OpenScape UC Application.

If you wish the conferences of the conference series to have a duration different from the default, specify the desired duration in the **Duration** column.

If the first conference of the conference series is to start at another time, specify the desired time in the **StartDate** column.

## **18.4 Logging the Coman Tool for Troubleshooting**

Each time you invoke the program, the Coman tool writes logging information in a log file in the working directory of the Coman tool.

The log file is called:

coman - log

## **18.5 Installing the Coman Tool**

The Coman tool is shipped with the product data carrier of OpenScape UC Application. You find it there in the following directory:

\support\Conferen

### **Installing the Coman Tool under Windows**

To install the Coman tool under Windows, copy the following file to a working directory that provides writing access.

- coman.jar

---

**NOTICE:** The Windows computer system used must be able to reach the application computer of OpenScape UC Application.

---

### Installing the Coman Tool under Linux

To install the Coman tool under Linux, copy the following files to a working directory that provides writing access.

- `coman.jar`
- `coman.sh`

---

**NOTICE:** The Linux computer system used must be able to reach the application computer of OpenScape UC Application.

---

## 18.6 Invoking the Coman Tool

The Coman tool is based on command lines. Each program invocation has the following general command format:

### Under Windows

`>java -jar coman.jar <action> <options, if required with parameters>`

*Example:* `>java -jar coman.jar initXLS -e Template-US -d US`

### Under Linux

`>coman.sh <action> <options, if required with parameters>`

*Example:* `>coman.sh initXLS -e Template-US -d US`

You can specify all options in long or short format.

*Example short format:* `>java -jar coman.jar initXLS -e Template-US -d US`

*Example long format:* `>java -jar coman.jar initXLS --exportFile Template-US --dateFormat US`

---

**NOTICE:** In the following description we exclusively use the Windows-based invocation. The Linux-based invocation results from this accordingly.

---

## 18.7 Invoking the Online Help of the Coman Tool

The Coman tool has an online help that describes all available commands.

Enter the following command to put out a list of all supported commands:

`>java -jar coman.jar -h`

Enter the following command to put out help information on a specific action:

`>java -jar coman.jar <action> -h`

The online help of the Coman tool is available in English language only.

## 18.8 Command Reference for the Coman Tool

The Coman tool supports the following actions.

- [createConferencePerDomainUsers](#)
- [deleteAll](#)
- [deleteConf](#)
- [deleteConfForUser](#)
- [exportDomainUsersToXLS](#)
- [exportDomainUsersWithPinsToXLS](#)
- [exportXLS](#)
- [getConfs](#)
- [importXLS](#)
- [initXLS](#)
- [scheduleConf](#)
- [startConf](#)
- [terminateConf](#)

In the following we describe all actions with their possible options and the options' parameters in detail.

### 18.8.1 createConferencePerDomainUsers

Creates a table in the Coman tool directory that contains as many conference entries as UC Application user accounts have been configured. Each of these conference entries determines an individual UC Application user account as conference creator.

Furthermore, a PIN is automatically defined for each conference. This PIN is derived from the ONS number of the associated user account.

After the table has been created, it is automatically imported in OpenScape UC Application via the [importXLS](#) action, which activates the relevant settings for OpenScape UC Application.

#### Command format

```
>java -jar coman.jar createConferencePerDomainUsers
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#e < file name > | ##exportFile < file name >)]
[(#l < number of digits > | ##extensionLength < number
of digits >)]
[(#pf < prefix > | ##prefix < prefix >)]
[(#pinl < audio PIN length > | ##audioPinLength < audio
PIN length >)]
```

*Example:*

```
>java -jar coman.jar createConferencePerDomainUsers -
s 10.10.10.1 -u ImExUser -p OscImEx13! -e OutputTable -l 66
```



| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost must be used.                                                                                                                                                                                                                                                            |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects access via the user account from the user.                                                                                                                                                                                                                                                                                                                                                 |
| --exportFile / -e        | Optional      | Defines the name of the exported table. The default setting is domainUsersyyyyMMdd_HHmmss.                                                                                                                                                                                                                                                                                                                                    |
| --extensionLength / -l   | Optional      | Defines the maximum number of extension digits. The specified number of extension digits must result in extensions that are unique for all configured extensions. The default setting is 4.                                                                                                                                                                                                                                   |
| --prefix / -pf           | Optional      | Defines a prefix with which the extension begins. This creates a conference PIN individual to the user account. The default setting is 00.                                                                                                                                                                                                                                                                                    |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 4.                                                                                                                                                                                                                                                                                                                                                       |

## 18.8.2 deleteAll

Deletes all conferences configured in the conference portal.

---

**IMPORTANT:** Conferences once deleted are irretrievably lost.

---

### Command format

```
>java -jar coman.jar deleteAll (
 -s < IP address > | --server < IP address >)
 (-u < user account ID > | --user < user account ID >)
```

```
(-p < password > | --password < password >)
```

*Example:*

```
>java -jar coman.jar deleteAll -s 10.10.10.1 -u ImExUser -p 0scImEx13!
```

| Option          | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s   | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u     | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |

### 18.8.3 deleteConf

Deletes in the conference portal a single conference via command line or several conferences by importing an import table.

---

**IMPORTANT:** Conferences once deleted are irretrievably lost.

---

#### Command format

```
>java -jar coman.jar deleteConf
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#pin < PIN > | ##confPin < PIN >)]
[(-i < name import file > | --importFile < name import file >)]
[(#pinl < length > | ##audioPinLength < length >)]
```

*Example:*

```
>java -jar coman.jar deleteConf -s 10.10.10.1 -u ImExUser -
p OscImEx13! -pin 1254
```

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --confPin / -pin         | Optional      | Defines the PIN of the conference to be deleted.                                                                                                                                                                                                                                                                                                                                                                              |
| --importFile / -i        | Optional      | Defines the name of the table that determines the conferences to be deleted.                                                                                                                                                                                                                                                                                                                                                  |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                       |

### 18.8.4 deleteConfForUser

Deletes in the conference portal all conferences for which a specific user account has been configured as creator.

---

**IMPORTANT:** Conferences once deleted are irretrievably lost.

---

#### Command format

```
>java -jar coman.jar deleteConfForUser
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
```

```
(-p < password > | --password < password >)
(-du < user account ID > | --deleteUser < user account ID >)
```

*Example:*

```
>java -jar coman.jar deleteConfForUser -s 10.10.10.1 -
u ImExUser -p 0scImEx13! -du mBrown@system
```

| Option             | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s      | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u        | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p    | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --deleteUser / -du | Mandatory     | Defines the ID of the user account for which the conferences are deleted. The relevant user account is not deleted.                                                                                                                                                                                                                                                                                                           |

## 18.8.5 exportDomainUsersToXLS

Creates a table in the Coman tool directory that contains as many conference entries as UC Application user accounts have been configured. Each of these conference entries determines an individual UC Application user account as conference creator.

---

**NOTICE:** **exportDomainUsersToXLS** does not create conferences but only the export table put out.

---

**Command format**

```
>java -jar coman.jar exportDomainUsersToXLS
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#e < file name > | ##exportFile < file name >)]
```

**Example:** >java -jar coman.jar exportDomainUsersToXLS -s 10.10.10.1 -u ImExUser -p 0scImEx13! -e OutputTable

| Option            | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s     | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u       | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p   | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --exportFile / -e | Optional      | Defines the name of the exported table. The default setting is domainUsersyyyyMMdd_HHmms.xls                                                                                                                                                                                                                                                                                                                                  |

### 18.8.6 exportDomainUsersWithPinsToXLS

Creates a table in the Coman tool directory that contains as many conference entries as UC Application user accounts have been configured. Each of these conference entries determines an individual UC Application user account as conference creator.

Furthermore, a PIN is automatically defined for each conference entry. This PIN is derived from the ONS number of the associated user account.

---

**NOTICE:** **exportDomainUsersWithPinsToXLS** does not create conferences but only the export table put out.

---

**Command format**

```
>java -jar coman.jar exportDomainUsersWithPinsToXLS
```

```
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#e < file name > | ##exportFile < file name >)]
[(#l < number of digits > | ##extensionLength < number
of digits >)]
[(#pf < prefix > | ##prefix < prefix >)]
[(#pinl < audio PIN length > | ##audioPinLength < audio
PIN length >)]
```

**Example:**

```
>java -jar coman.jar exportDomainUsersWithPinsToXLS -
s 10.10.10.1 -u ImExUser -p 0scImEx13! -e OutputTable
```

| Option                 | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s          | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u            | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p        | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --exportFile / -e      | Optional      | Defines the name of the exported table. The default setting is domainUsersyyyyMMdd_HHmmss.xls                                                                                                                                                                                                                                                                                                                                 |
| --extensionLength / -l | Optional      | Defines the maximum number of extension digits. The specified number of extension digits must result in extensions that are unique for all configured ONS numbers. The default setting is 4.                                                                                                                                                                                                                                  |
| --prefix / -pf         | Optional      | Defines a prefix with which the unique extension begins. This creates a conference PIN individual to the user account. The default setting is 00.                                                                                                                                                                                                                                                                             |

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --audioPinLength / -pinl | Optional      | <p>Defines the PIN length for audio conferences. The default setting is 6.</p> <hr/> <p><b>NOTICE:</b> In principle, the PIN length results from the length of the defined prefix (-pf) and the extension length (-l). If the value of -pinl is smaller than the sum of -pf and -l, Coman uses fewer digits of the defined prefix accordingly. If the value of -pinl is greater than the sum of -pf and -l, Coman uses the digits of the defined prefix several times until the desired PIN length (-pinl) has been reached.</p> <hr/> |

## 18.8.7 exportXLS

Exports the data of all existing conferences to an export table. The single table entries are sorted by ascending PIN by default.

### Command format

```
>java -jar coman.jar exportXLS
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#e < file name > | ##exportFile < file name >)]
[(#pinl < length > | ##audioPinLength < length >)]
[(#d < date format > | ##dateFormat < date format >)]
[(#o < column number > | ##orderBy < column number >)]
```

### Example:

```
>java -jar coman.jar exportXLS -s 10.10.10.1 -u ImExUser -
p OscImEx13! -o 0
```

| Option        | Specification |                                                                                                                                                                          |
|---------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s | Mandatory     | <p>Defines the IP address of the application computer of OpenScope UC Application. If you execute the Coman tool on the application computer, localhost can be used.</p> |

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --user / -u              | Mandatory     | <p>Defines the ID of the user account that the Coman tool uses for logging on to the OpenScope system. At least the following user profiles must have been assigned to the deployed user account:</p> <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                                      |
| --exportFile / -e        | Optional      | Defines the name of the exported table. The default setting is conferencesyyyyMMdd_HHmmss.xls                                                                                                                                                                                                                                                                                                                                        |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                              |
| --dateFormat / -d        | Optional      | <p>Defines the format in which the Coman tool interprets the date specifications in the table. Possible parameters are:</p> <ul style="list-style-type: none"> <li>• DE – d.M.yy HH:mm</li> <li>• US – M/d/yy HH:mm</li> </ul> <p>The default setting is DE.</p>                                                                                                                                                                     |
| --orderBy / -o           | Optional      | <p>Defines the number of the table column by which the table entries are sorted. The first table column has number 0. The default setting is 5. As a result, the table entries are sorted by the table column <b>AudioPin</b>.</p>                                                                                                                                                                                                   |

## 18.8.8 getConfs

Exports the data of selected conferences to an export table. The exported table entries are sorted by ascending PIN.

Parameters determine during the command invocation from which conferences data is exported.

### Command format

```
>java -jar coman.jar getConfs
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
```



```
[(#c < user account ID > |##creator < user account ID
>)]
[(#in < time > |##invitee < time >)]
[(#st < time > |##startTime < time >)]
[(#et < time > |##endTime < time >)]
[(#oc < Boolean > |##orphaned < Boolean >)]
[(#e < file name > |##exportFile < file name >)]
[(#pinl < length > |##audioPinLength < length >)]
[(#d < date format > |##dateFormat < date format >)]
```

**Example:**

```
>java -jar coman.jar getConfs -s 10.10.10.1 -u ImExUser -
p 0scImEx13! -st 070410 -d DE
```

| Option            | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s     | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u       | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p   | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --creator / -c    | Optional      | Defines the ID of a user account. Only the conferences created by the associated user are exported.                                                                                                                                                                                                                                                                                                                           |
| --invitee / -in   | Optional      | Defines the ID of a user account. Only the conferences for which the associated user has been invited are exported.                                                                                                                                                                                                                                                                                                           |
| --startTime / -st | Optional      | Defines the start of a time interval. Only the conferences that begin within this interval are exported. If you specify this parameter, you need to specify the parameters -d and -et also.                                                                                                                                                                                                                                   |

| Option                   | Specification |                                                                                                                                                                                                                                                    |
|--------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --endTime / -et          | Optional      | Defines the end of a time interval. Only the conferences that begin within this interval are exported. If you specify this parameter, you need to specify the parameters -d and -st also.                                                          |
| --orphaned / -oc         | Optional      | Defines that only conferences of creators for whom no user account exists any more are exported. This option does not use any parameters.                                                                                                          |
| --exportFile / -e        | Optional      | Defines the name of the exported table. The default setting is conferencesyyyyMMdd_HHmms.xls                                                                                                                                                       |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                            |
| --dateFormat / -d        | Optional      | Defines the format in which the Coman tool interprets the date specifications in the table. Possible parameters are: <ul style="list-style-type: none"> <li>• DE – d.M.yy HH:mm</li> <li>• US – M/d/yy HH:mm</li> </ul> The default setting is DE. |

## 18.8.9 importXLS

Imports a table with conference information in OpenScope UC Application. If a conference to be exported exists already and the overwriting option is active, the relevant conference data is updated.

After the import, the Coman tool generates a result table that documents all created and updated conferences. Its name is displayed in the command line under **exportFile**.

If an error occurs during the import for a conference, it is put out in the result table at the end of the table row of the relevant conference.

### Command format

```
>java -jar coman.jar importXLS
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
(-i < import file name > | -- importFile < import file name >)
[(#d < date format > | ##dateFormat < data format >)]
[(#pinl < length > | ##audioPinLength < length >)]
[(#e < file name > | ##exportFile < file name >)] [(-
ow | ##overwrite)]
```

*Example:*

```
>java -jar coman.jar importXLS -s 10.10.10.1 -u ImExUser -
p OscImEx13! -i Import2510
```

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --importFile / -i        | Mandatory     | Defines the name of the table the data of which is to be imported.                                                                                                                                                                                                                                                                                                                                                            |
| --overwrite / -ow        | Optional      | Defines that the data of an existing conference may be overwritten by the data of the import table. This option does not use any parameters.                                                                                                                                                                                                                                                                                  |
| --dateFormat / -d        | Optional      | Defines the format in which the Coman tool interprets the date specifications in the table. Possible parameters are: <ul style="list-style-type: none"> <li>• DE – d.M.yy HH:mm</li> <li>• US – M/d/yy HH:mm</li> </ul> The default setting is DE.                                                                                                                                                                            |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                       |
| --exportFile / -e        | Optional      | Defines the name of the exported table. The default setting is conferencesyyyyMMdd_HH:mm:ss.xls                                                                                                                                                                                                                                                                                                                               |

## 18.8.10 initXLS

Creates in the Coman tool directory an empty table with all available columns. This table can be used as format template for importing data in OpenScape UC Application using the Coman tool.

**Command format**

```
>java -jar coman.jar initXLS
[(#e < export file name > |##exportFile < export file
 name >)]
[(#d < date format > |##dateFormat < date format >)]
```

*Example:*

```
>java -jar coman.jar initXLS -e Template-US -d US
```

| parameter         | Specification |                                                                                                                                                                                                                                                       |
|-------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --exportFile / -e | Optional      | Defines the file name incl. suffix for the created table.<br><br>The file name of a created table reads by default:<br>template<date>-<time>.xls                                                                                                      |
| --dateFormat / -d | Optional      | Defines the format in which the Coman tool interprets the date specifications in the table.<br>Possible parameters are: <ul style="list-style-type: none"> <li>• DE – d.M.yy HH:mm</li> <li>• US – M/d/yy HH:mm</li> </ul> The default setting is DE. |

**18.8.11 scheduleConf**

Schedules in the conference portal a single conference via command line or several conferences by importing an import table.

**Command format**

```
>java -jar coman.jar scheduleConf
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#pin < PIN > |##confPin < PIN >)]
[(--i < import file name > | --importFile < import file
 name >)]
[(#pinl < length > |##audioPinLength < length >)]
```

*Example:*

```
>java -jar coman.jar scheduleConf -s 10.10.10.1 -u ImExUser
-p OscImEx13! -pin 1254
```

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --confPin / -pin         | Optional      | Defines the PIN of the conference to be scheduled.                                                                                                                                                                                                                                                                                                                                                                            |
| --importFile / -i        | Optional      | Defines the name of the table that determines the conferences to be scheduled.                                                                                                                                                                                                                                                                                                                                                |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                       |

## 18.8.12 startConf

Starts a single conference via command line or several conferences by importing an import table.

### Command format

```
>java -jar coman.jar startConf
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
[(#pin < PIN > | ##confPin < PIN >)]
[(--i < import file name > | --importFile < import file name >)]
[(#pinl < length > | ##audioPinLength < length >)]
```

*Example:*

```
>java -jar coman.jar startConf -s 10.10.10.1 -u ImExUser -p 0scImEx13! -pin 1254
```

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --confPin / -pin         | Optional      | Defines the PIN of the conference to be started.                                                                                                                                                                                                                                                                                                                                                                              |
| --importFile / -i        | Optional      | Defines the name of the table that determines the conferences to be started.                                                                                                                                                                                                                                                                                                                                                  |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                       |

## 18.8.13 terminateConf

Ends a single conference via command line or several conferences by importing an import table.

### Command format

```
>java -jar coman.jar terminateConf
(-s < IP address > | --server < IP address >)
(-u < user account ID > | --user < user account ID >)
(-p < password > | --password < password >)
```

```
[(#pin < PIN > | ##confPin < PIN >)]
[(--i < import file name > | --importFile < import file
 name >)]
[(#pinl < length > | ##audioPinLength < length >)]
```

*Example:*

```
>java -jar coman.jar terminateConf -s 10.10.10.1 -
u ImExUser -p OscImEx13! -pin 1254
```

| Option                   | Specification |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --server / -s            | Mandatory     | Defines the IP address of the application computer of OpenScape UC Application. If you execute the Coman tool on the application computer, localhost can be used.                                                                                                                                                                                                                                                             |
| --user / -u              | Mandatory     | Defines the ID of the user account that the Coman tool uses for logging on to the OpenScape system. At least the following user profiles must have been assigned to the deployed user account: <ul style="list-style-type: none"> <li>• <b>Administrator</b> (Symphonia application)</li> <li>• <b>Customer Administrator</b> (Symphonia application)</li> <li>• <b>Service Technician</b> (Symphonia application)</li> </ul> |
| --password / -p          | Mandatory     | Defines the password that protects the access via the user account from --user.                                                                                                                                                                                                                                                                                                                                               |
| --confPin / -pin         | Optional      | Defines the PIN of the conference to be ended.                                                                                                                                                                                                                                                                                                                                                                                |
| --importFile / -i        | Optional      | Defines the name of the table that determines the conferences to be ended.                                                                                                                                                                                                                                                                                                                                                    |
| --audioPinLength / -pinl | Optional      | Defines the PIN length for audio conferences. The default setting is 6.                                                                                                                                                                                                                                                                                                                                                       |

## 19 OpenScape Auto Attendant

This chapter provides information about the following topics of the OpenScape Auto Attendant plug-in:

- [Function of the OpenScape Auto Attendant](#)
- [Opening the OpenScape Auto Attendant Configuration](#)
- [Configuring Auto Attendant Profiles](#)
- [General Settings of Auto Attendant Profiles](#)
- [Error Handling Settings of Auto Attendant Profiles](#)
- [Resource Settings of Auto Attendant Profiles](#)
- [Operation Mode Settings of Auto Attendant Profiles](#)
- [Keypad Layout Settings of the Operation Modes](#)
- [Configuration via Administrator Access](#)
- [Configuring a Routing Workflow](#)

### 19.1 Function of the OpenScape Auto Attendant

The OpenScape Auto Attendant is an automated central postmaster account that can be customized.

With its help you can construct static and interactive routing workflows from pre-defined modules in a simple way. Such workflows can route incoming calls time- and caller-controlled without an employee having to interfere in the routing process.

### 19.2 Opening the OpenScape Auto Attendant Configuration

You can perform the most important OpenScape Auto Attendant settings specific to the Media Server in the OpenScape Auto Attendant plug-in of the - Common Management Platform. This configuration is based on Auto Attendant profiles of which several may exist and each represents an individually designed routing workflow.

How to open the configuration dialog of the OpenScape Auto Attendant plug-in:

- 1) On the **Configuration** navigation tab of the Common Management Platform click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select the **AutoAttendant** link in the list.



The configuration dialog of the application OpenScape Auto Attendant opens. You see a list of all Auto Attendant profiles configured in the selected OpenScape Media Server.

## 19.3 Configuring Auto Attendant Profiles

Every Auto Attendant profile represents an individually designed routing workflow that can realize the following two accesses:

- A **user access** Calls via the user access are routed according to the associated workflow.

---

**NOTICE:** Every routing workflow has exactly one user access.

---

- An **administrator access** Provides a telephone user interface for configuring selected settings of the associated routing workflow. [Configuration via Administrator Access](#) on page 812 describes the configuration options that the administrator access provides.

---

**NOTICE:** An administrator access is always available for the routing workflow of the default profile **start**. The administrator access is optional for all other routing workflows.

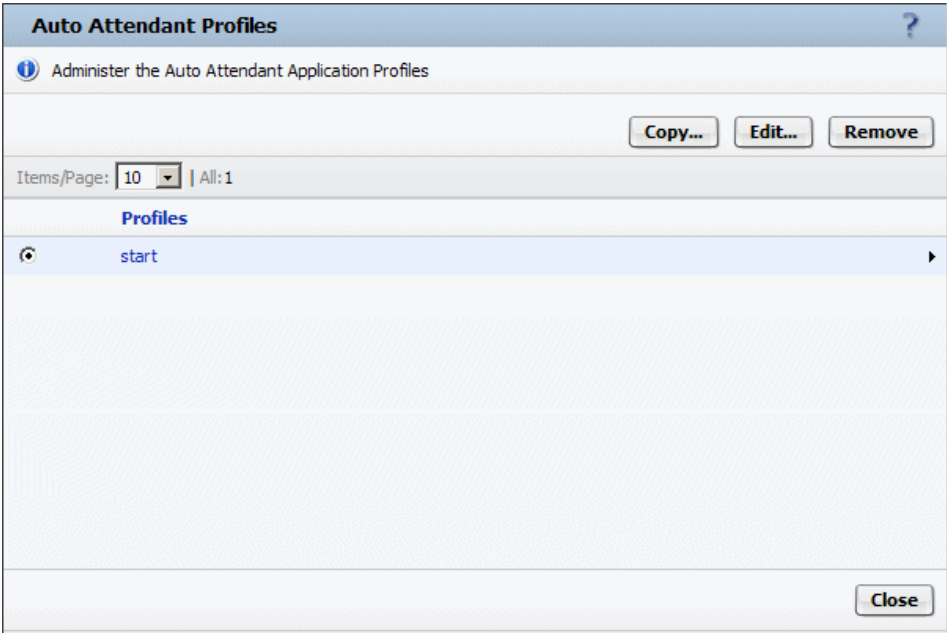
---

With the help of a Media Server terminal you need to assign an individual phone number to each user and administrator access to make them reachable to callers.

The settings of an Auto Attendant profile are divided in the following areas:

- Universal settings
- Settings for error handling
- Settings for the operation modes
- Settings for the resources

After the OpenScape Auto Attendant installation the **start** profile is pre-configured by default.



You can use the following buttons for managing the Auto Attendant profiles:

**Copy**

Opens the configuration dialog for a new Auto Attendant profile. The pre-configured settings correspond to those of the Auto Attendant profile selected in the profile list.

**Edit**

Opens the configuration dialog for the Auto Attendant profile selected in the profile list.

**Remove**

Deletes the Auto Attendant profile selected in the profile list. You cannot delete the pre-configured Auto Attendant profile **start**.

19.4 General Settings of Auto Attendant Profiles

On the **General** tab of the profile settings you configure basic settings for the relevant routing workflow.

|                                |                                                      |
|--------------------------------|------------------------------------------------------|
| <b>General Settings</b>        |                                                      |
| Default language:              | <input type="text" value="English (United States)"/> |
| Symphonia domain:              | <input type="text" value="system"/>                  |
| Address translation context:   | <input type="text" value=""/>                        |
| Transfer timeout (in seconds): | <input type="text" value="30"/>                      |
| <b>Administrator Access</b>    |                                                      |
| Administrator access PIN:      | <input type="text" value="1234"/>                    |

**Default language**

|                         |                                                                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Default:</i>         | English (US)                                                                                                                                                                                                                                          |
| <i>Possible values:</i> | <ul style="list-style-type: none"> <li>• German</li> <li>• English (UK)</li> <li>• English (US)</li> <li>• Spanish</li> <li>• French</li> <li>• Italian</li> <li>• Portuguese (Brazil)</li> <li>• Portuguese (Portugal)</li> <li>• Chinese</li> </ul> |
| <i>Remark:</i>          | Only those languages are offered for selection that have been installed for the language package.                                                                                                                                                     |

Defines the language in which the OpenScape Auto Attendant plays greetings to callers.

**Symphonia domain**

*Default:* system

*Remark:* Cannot be modified.

**Address translation context**

*Default:* <default context>

*Possible values:* <ID of an address translation context>

If e.g. a caller needs to specify a phone number, he/she will do this always with reference to the respective location. For example, as pure extension or as phone number with area code but without international prefix. But this leads to problems if the OpenScape Auto Attendant e.g. is located in a country different from the caller's.

To evade such phone number problems, the OpenScape system transforms all phone numbers before the actual processing into a normalized phone number format – e. g. +492404901100. The thus normalized phone numbers then contain all information that the phone number uniquely identifies or localizes. The OpenScape system uses so-called address translation contexts for normalizing phone numbers.

**Address translation context** defines the ID of an address translation context configured in the CMP. The OpenScape Auto Attendant uses this context for phone number normalization.

**Transfer timeout**

*Default:* 30 [seconds]

*Possible values:* <Time> [seconds]

Defines for the following OpenScape Auto Attendant actions how long the attempt is made to set up a connection to the desired subscriber.

- [Transfer to an Extension](#)
- [Enter an Extension to be transferred to](#)

If the connection fails, the user returns to the OpenScape Auto Attendant main menu.

#### **Activating the administrator mode**

*Default:* <activated>

*Remark:* Is not displayed for the default profile **start**.

Defines whether an administrator access is to be available for the relevant routing workflow. An administrator access is always available for the routing workflow of the default profile **start**.

#### **PIN for the administrator access**

*Default:* 1234

*Possible values:* <digit sequence>

Defines the PIN that protects the administrator access of the relevant routing workflow from unauthorized access.

## **19.5 Error Handling Settings of Auto Attendant Profiles**

On the **Error Handling** tab of the profile settings you configure how the relevant routing workflow reacts to incorrect entries by callers.

| Error Handling                                 |                                     |
|------------------------------------------------|-------------------------------------|
| Number of repetitions (wrong / missing input): | <input type="text" value="3"/>      |
| Call operator in case of error:                | <input checked="" type="checkbox"/> |
| Operator number                                | <input type="text" value="200"/>    |

#### **Number or repetitions (wrong / missing input)**

*Default:* 3

*Possible values:* <Number>

Defines how often a greeting can be consecutively played if a caller uses incorrect entries or does not react to input prompts at all. When the specified number of repetitions is exceeded, the connection is closed or the caller is connected to an operator – cf. [Call operator in case of error](#).

#### **Call operator in case of error**

*Default:* <deactivated>

If a caller makes incorrect user entries or does not react to input prompts at all, the connection can be closed or the caller be connected to an operator.

If **Call operator in case of error** is inactive, the connection is closed; if the option is active, the caller is connected to an operator. This all happens if [Number or repetitions \(wrong / missing input\)](#) is exceeded.

The operator number is determined under [Operator number](#).

#### **Operator number**

*Default:* -

*Possible values:* <Calling number>

*Remark:* Is only displayed if [Call operator in case of error](#) is active.

Defines a subscriber's phone number. A call is routed to this subscriber with exceeded [Number or repetitions \(wrong / missing input\)](#) and active [Call operator in case of error](#) option.

## 19.6 Resource Settings of Auto Attendant Profiles

On the **Resources** tab of the profile settings you manage the greetings for the user and administrator access of the relevant routing workflow.

| Items/Page: 10   All: 120   1   << >>                                  |                                                       |             | <a href="#">Edit...</a> <a href="#">Search...</a> |
|------------------------------------------------------------------------|-------------------------------------------------------|-------------|---------------------------------------------------|
| Prompt ID                                                              | Alternate Text                                        | Description |                                                   |
| <input type="radio"/> adminMenu.activateCompanyVacation                | To activate the business hours mode and the compan... |             | ▶                                                 |
| <input checked="" type="radio"/> adminMenu.activateCompanyVacationHelp | ...activate the business hours and the company vac... |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateEmergency                      | To activate the emergency mode, push 6.               |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateEmergencyHelp                  | ...activate the emergency mode,...                    |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateModeMenu.activateAll           | To activate all modes, push 1.                        |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateModeMenu.activateAllHelp       | ...activate all modes, ...                            |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateModeMenu.activateOne           | To change the active mode, push 2.                    |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateModeMenu.activateOneHelp       | ...change the active mode.                            |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateModeMenu.allModesActivated     | All modes are now active.                             |             | ▶                                                 |
| <input type="radio"/> adminMenu.activateOffHours                       | To activate the business hours mode and the non-bu... |             | ▶                                                 |

The following buttons are available to manage greetings for the user and administrator access of the relevant routing workflow:

### Edit

Opens an import dialog for loading an individual greeting for the selected prompt ID. This new greeting then replaces the greeting played so far.

### Search

Opens a search dialog in which you can browse available greetings for an individual search item.

## 19.7 Operation Mode Settings of Auto Attendant Profiles

On the **Operation Modes** tab you configure the routing workflow according to which the OpenScape Auto Attendant routes incoming calls.

The configured operation modes define how the workflow operates. One of the following operation modes can be used for each Auto Attendant profile.

- [Business Hours](#)
- [Outside Business Hours](#)
- [Weekend](#)
- [Public Holidays](#)
- [Company Vacation](#)
- [Emergency](#)

| Operation Modes                                                      |  |
|----------------------------------------------------------------------|--|
| <div><div></div><div>Add</div><div>Edit</div><div>Remove</div></div> |  |
| Items/Page: 10   All: 4                                              |  |
| Operation Mode                                                       |  |
| <div><div></div>Business hours</div>                                 |  |
| <div><div></div>Public Holidays</div>                                |  |
| <div><div></div>Weekend</div>                                        |  |
| <div><div></div>Non-Business Hours</div>                             |  |

You can use the following buttons for managing the operation modes for an Auto Attendant profile:

**Add**

Opens a selection dialog for adding a new operation mode to the routing workflow. You can only select operation modes that have not yet been used for the relevant Auto Attendant profile.

**Edit**

Opens the configuration dialog for the operation mode selected in the operation mode list.

**Remove**

Deletes the operation mode selected in the operation mode list.

19.7.1 Business Hours

For the **Business Hours** operation mode you can determine a continuous period per weekday that represents opening hours. Furthermore, you can use a keypad layout to determine how the routing workflow reacts to entries via keypad during the defined business hours.

**NOTICE:** If you wish to exclude time definitions from the **Business Hours** operation mode, you need to represent them by other operation modes – e.g. by the **Weekend** operation mode. If weekdays remain unconsidered during the configuration of an Auto Attendant profile, a note informs you accordingly when you save your settings. The OpenScape Auto Attendant uses the **Business Hours** operation mode for unconsidered days by default.

**NOTICE:** You can control the setting for the option **Business hours mode is active** via the telephone user interface of the associated administrator access.

Business Times

Business hours mode is active. ☒

Sel: 5 | Items/Page: 10 | All: 7

| Business Days                                 | Business Hours Start | Business Hours End |
|-----------------------------------------------|----------------------|--------------------|
| <input checked="" type="checkbox"/> Monday    | 08 : 00              | 17 : 00            |
| <input checked="" type="checkbox"/> Tuesday   | 08 : 00              | 17 : 00            |
| <input checked="" type="checkbox"/> Wednesday | 08 : 00              | 17 : 00            |
| <input checked="" type="checkbox"/> Thursday  | 08 : 00              | 17 : 00            |
| <input checked="" type="checkbox"/> Friday    | 08 : 00              | 17 : 00            |
| <input type="checkbox"/> Saturday             | 00 : 00              | 00 : 00            |
| <input type="checkbox"/> Sunday               | 00 : 00              | 00 : 00            |

Keypad Layout

Add...Edit...Remove...

Items/Page: 10 | All: 5

| DTMF-Key                | Action                                  |
|-------------------------|-----------------------------------------|
| <input type="radio"/> 1 | Transfer to an extension                |
| <input type="radio"/> 2 | Send a message to                       |
| <input type="radio"/> 3 | Hangup                                  |
| <input type="radio"/> 4 | Select a contact to be transferred to   |
| <input type="radio"/> 5 | Enter an extension to be transferred to |

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

19.7.2 Outside Business Hours

Applicable weekdays and times for the **Non-Business Hours** operation mode result from the time settings of the **Business hours** operation mode.

If you activate the option **Keypad Layout Menu for the non-business hours**, you can use a keypad layout to also define how the routing workflow reacts to entries via keypad outside of business hours.

If no keypad layout has been defined, the caller hears a non-business-hours greeting and the connection is closed.

**NOTICE:** You can control the setting for the option **Non-business hours mode is active** via the telephone user interface of the associated administrator access.

The non-business hours mode is active on the defined business days, outside the business hours.

Non-business hours mode is active.

☒

Items/Page: 10 | All: 5

| Business Days | Business Hours Start | Business Hours End |
|---------------|----------------------|--------------------|
| Monday        | 08:00                | 17:00              |
| Tuesday       | 08:00                | 17:00              |
| Wednesday     | 08:00                | 17:00              |
| Thursday      | 08:00                | 17:00              |
| Friday        | 08:00                | 17:00              |

Keypad Layout Menu for the non-business hours

☒

Keypad Layout

Add...Edit...Remove

Items/Page: 10 | All: 1

| DTMF-Key | Action                   |
|----------|--------------------------|
| 9        | Transfer to an extension |

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

19.7.3 Weekend

The weekdays that are possible for the **Weekend** operation mode result from the day settings of the **Business hours** operation mode. From the days that do not belong to the **Business hours** operation mode you can select the days to be assigned to the **Weekend** operation mode.

If you activate the option **Keypad Layout Menu for the weekend**, you can use a keypad layout to also define how the routing workflow reacts to entries via keypad during weekend times.

If no keypad layout has been defined, the caller hears a weekend greeting and the connection is closed.

**NOTICE:** You can control the setting for the option **Weekend mode is active** via the telephone user interface of the associated administrator access.



Configure the days for the weekend

Weekend mode is active. ☒

Sel:0 | Items/Page: 10 | All:2

Weekend

☒ Saturday

☒ Sunday

Keypad Layout Menu for the weekend ☒

Keypad Layout

Add...Edit...Remove

Items/Page: 10 | All:1

| DTMF-Key | Action                   |
|----------|--------------------------|
| 9        | Transfer to an extension |

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

### 19.7.4 Public Holidays

You can specify individual day-based periods for the **Public Holidays** operation mode.

If you activate the option **Keypad Layout Menu**, you can use a keypad layout to also define how the routing workflow reacts to entries via keypad during the specified public holidays.

If no keypad layout has been defined, the caller hears a public-holiday greeting and the connection is closed.

The operation mode **Public Holidays** does not become active until the option **Public holidays mode is active** has been enabled.

**NOTICE:** You can control the setting for the option **Public holidays mode is active** via the telephone user interface of the associated administrator access.

Configure the date ranges for the public holidays

Public holidays mode is active.

☒

Add...

Remove

Items/Page: 10 | All: 0

| Start date | End date |
|------------|----------|
|------------|----------|

Keypad Layout Menu

☒

Keypad Layout

Add...

Edit...

Remove

Items/Page: 10 | All: 1

| DTMF-Key | Action |
|----------|--------|
| 9        | Hangup |

You can use the following buttons for managing individual public holiday periods:

**Add**

Adds a new entry with empty date fields to the date list. You can then set the content of the single date fields.

**Remove**

Deletes the entry you have selected in the date list.

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

19.7.5 Company Vacation

You can create individual day-based periods for the **Company Vacation** operation mode.

If you activate the option **Keypad Layout Menu**, you can use a keypad layout to also define how the routing workflow reacts to entries via keypad during the specified company vacation.

If no keypad layout has been defined, the caller hears a company vacation greeting and the connection is closed.

The operation mode **Company Vacation** is not active until the option **Company vacation mode is active** has been enabled.

**NOTICE:** You can control the setting for the option **Company vacation mode is active** via the telephone user interface of the associated administrator access.

**Configure the date ranges for the company vacation**

Company vacation mode is active. ☒

[Add...](#) [Remove](#)

Items/Page: 10 | All: 1

| Start date   | End date     |
|--------------|--------------|
| 01 July 2011 | 01 July 2011 |

Keypad Layout Menu ☒

**Keypad Layout**

[Add...](#) [Edit...](#) [Remove](#)

Items/Page: 10 | All: 1

| DTMF-Key | Action                   |
|----------|--------------------------|
| 9        | <a href="#">Playback</a> |

You can use the following buttons for managing individual company vacation periods:

#### Add

Adds a new entry with empty date fields to the date list. You can then set the content of the single date fields.

#### Remove

Deletes the entry you have selected in the date list.

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

## 19.7.6 Emergency

You cannot configure any restricting periods for the operation mode **Emergency**. As soon as this operation mode has been enabled with the option **Emergency mode is active**, it is prioritized against all other configured operation modes.

You can use the following options for determine, how the operation mode **Emergency** reacts to entries via keypad.

- **Hangup after emergency announcement**

In this case the caller only hears an emergency announcement. Subsequently, the connection is closed. The routing workflow does not process any entries made via keypad.

- **Activate the Keypad Layout Menu for emergency**  
In this case you can use an individual keypad layout to define for the operation mode **Emergency** how the routing workflow reacts to entries via keypad.
- **Activate the Business Hours Menu**  
In this case the routing workflow reacts to entries via keypad as has been defined in the keypad layout of the operation mode **Business Hours**.

**NOTICE:** You can control the setting for the option **Emergency mode is active** via the telephone user interface of the associated administrator access.

Configure the emergency mode

Emergency mode is active.  
All other modes will be inactive.

☒

Menu behaviour

Activate the Keypad Layout Menu for emergency

Keypad Layout

Add...Edit...Remove

Items/Page: 10 | All: 1

| DTMF-Key                           | Action   |
|------------------------------------|----------|
| <div><input type="radio"/></div> 9 | Playback |

[Keypad Layout Settings of the Operation Modes](#) on page 808 provides detailed information about the keypad layout.

## 19.8 Keypad Layout Settings of the Operation Modes

You can define how a routing workflow reacts to entries via keypad for all available operation modes. To this, you can configure a so-called keypad layout for each operation mode.

Keypad Layout

Add...Edit...Remove

Items/Page: 10 | All: 5

| DTMF-Key                           | Action                                  |
|------------------------------------|-----------------------------------------|
| <div><input type="radio"/></div> 1 | Transfer to an extension                |
| <div><input type="radio"/></div> 2 | Send a message to                       |
| <div><input type="radio"/></div> 3 | Hangup                                  |
| <div><input type="radio"/></div> 4 | Select a contact to be transferred to   |
| <div><input type="radio"/></div> 5 | Enter an extension to be transferred to |

Each keypad layout can contain up to nine entries. Each of these entries consists of an assignment of DTMF key and Auto Attendant action.

You can select the keys **1** to **9** to assign any of the following Auto Attendant actions to one of them:

- [Transfer to an Extension](#)

- [Transfer to an Extension \(blind Transfer\)](#)
- [Hangup](#)
- [Enter an Extension to be transferred to](#)
- [Enter an Extension to be transferred to \(blind Transfer\)](#)
- [Select a Contact to be transferred to](#)
- [Send a Message to](#)
- [Playback](#)

You can use the following buttons for managing a keypad layout:

#### Add

Opens a configuration dialog for creating a new assignment of DTMF key and action.

#### Edit

Opens the configuration dialog for the key-action assignment selected in the keypad layout list.

#### Remove

Deletes the key-action assignment selected in the keypad layout list.

## 19.8.1 Transfer to an Extension

This Auto Attendant action enables the caller to have himself/herself connected to a defined subscriber. If this subscriber cannot be reached, alternative ones can be defined.

OpenScape Auto Attendant attempts to connect the caller to the first subscriber of the list. If this attempt fails, it tries to connect the caller to the second subscriber of the list, etc.

If the caller cannot be routed to any of the subscribers, he/she returns to the OpenScape Auto Attendant main menu.

The screenshot shows the configuration interface for the 'Transfer to an extension' action. At the top, there is a 'DTMF Key' dropdown set to '1' and an 'Auto Attendant Action' dropdown set to 'Transfer to an extension'. Below this is a section titled 'Configure the option to call an extension.' with 'Add...' and 'Remove' buttons. A table below shows the list of subscribers with columns for 'Transfer Destination' and 'Transfer Announcement'.

|                       | Transfer Destination | Transfer Announcement |
|-----------------------|----------------------|-----------------------|
| <input type="radio"/> | +4924043411234       | support               |
| <input type="radio"/> | +4924043415678       | helpdesk              |

The following settings must be performed for every subscriber:

- **Transfer Destination**  
Specifies the phone number of the subscriber who may have to be the routing target.
- **Transfer Announcement**  
Specifies the information text to be played to the caller for the routing target.

19.8.2 Transfer to an Extension (blind Transfer)

This Auto Attendant action enables the caller to have himself/herself connected to a defined subscriber. However, the OpenScape Auto Attendant does not monitor whether this routing is successful.

If the routing fails, the OpenScape Auto Attendant closes the connection to the caller.

DTMF Key

1

Auto Attendant Action

Transfer to an extension (blind transfer)

Configure the option to call an extension.

Items/Page: 10 | All: 2

| Transfer Destination | Transfer Announcement |
|----------------------|-----------------------|
| +4924043411234       | support               |
| +4924043415678       | helpdesk              |

You need to perform the following settings for this action:

- Transfer Destination**  
Specifies the phone number of the subscriber who is to be the routing target.
- Transfer Announcement**  
Specifies the information text to be played to the caller for the routing target.

19.8.3 Hangup

This Auto Attendant action closes the connection to the caller without any previous prompts.

19.8.4 Enter an Extension to be transferred to

This Auto Attendant action routes the caller to an extension that he/she needs to enter via the keypad of his/her telephone. The OpenScape Auto Attendant is in control of the routing.

If the routing fails, the caller returns to the OpenScape Auto Attendant main menu.

DTMF Key

5

Auto Attendant Action

Enter an extension to be transferred to

Configure the option to transfer to an entered extension

Maximum extension length

5

You need to configure the maximum length of this phone number for this action under **Maximum extension length**.

### 19.8.5 Enter an Extension to be transferred to (blind Transfer)

This action routes the caller to an extension that he/she needs to enter via the keypad of his/her telephone. However, the OpenScape Auto Attendant does not monitor whether this routing is successful.

If the routing fails, the OpenScape Auto Attendant closes the connection to the caller.

The screenshot shows a configuration form for the 'Enter an extension to be transferred to (blind transfer)' action. It includes a 'DTMF Key' dropdown set to '9', an 'Auto Attendant Action' dropdown set to 'Enter an extension to be transferred to (blind transfer)', and a section titled 'Configure the option to transfer to an entered extension' with a 'Maximum extension length' input field set to '3'.

You need to configure the maximum length of this phone number for this action under **Maximum extension length**.

### 19.8.6 Select a Contact to be transferred to

This Auto Attendant action enables the caller to have himself/herself connected to a contact from the OpenScape user database. The caller needs to enter the name of the desired contact via the letters of the telephone keypad.

### 19.8.7 Send a Message to

This Auto Attendant action enables the caller to leave a voice message. This voice message is then sent to a defined e-mail address.

The screenshot shows a configuration form for the 'Send a message to' action. It includes a 'DTMF Key' dropdown set to '2', an 'Auto Attendant Action' dropdown set to 'Send a message to', and a section titled 'Configure the option to send a message.' Below this is a table with two columns: 'Destination' and 'Announcement'. The 'Destination' column contains the email address 'mail@company.com', and the 'Announcement' column contains the text 'support'.

| Destination      | Announcement |
|------------------|--------------|
| mail@company.com | support      |

You need to perform the following settings for this action:

- **Destination**  
Specifies the e-mail address to which a voice message is sent that a caller leaves.
- **Announcement**  
Specifies the information text to be played to the caller for the destination.

## 19.8.8 Playback

This Auto Attendant action enables you to play an individual greeting to the caller.

The screenshot shows the configuration page for the 'Playback' action. At the top, there is a 'DTMF Key' dropdown menu set to '9' and an 'Auto Attendant Action' dropdown menu set to 'Playback'. Below these is a section titled 'Configure the playback prompts.' with a descriptive paragraph: 'The playback menu prompt is announced in the Auto Attendant menu to offer the playback prompt and the key to be pushed. The ",push <dtmf key>" prompt is added automatically at the end of the playback menu prompt. If the offered key is pushed, the playback prompt will be played back.' There are two main sections for configuration: 'Playback menu prompt' and 'Playback Prompt'. Each section has a 'Text' input field, a checkbox for 'Use uploaded prompt', and an 'Upload Prompt...' button. Below each checkbox is a file upload area.

For this action you need to define the following two greeting prompts:

- **Playback menu prompt**

This prompt is played to the caller in the main menu so that he/she can select the appropriate playback action.

- **Playback Prompt**

This prompt is played to the caller in the main menu after he/she has selected the appropriate playback action.

You need to perform one of the following settings for each of the two prompts:

- **Text**

Specifies the prompt to be played in text form. This text is then played to the caller via the text-to-speech feature.

- **Use uploaded prompt**

Specifies the prompt to be played by a sound file played to the caller. Using the **Upload Prompt** button you can upload the desired sound file to the OpenScape Auto Attendant.

## 19.9 Configuration via Administrator Access

You can activate or deactivate the configured operation modes of a routing workflow via the telephone user interface of the administrator access. Furthermore, you can record an emergency greeting for the [Emergency](#) operation mode.

An administrator access is always available for the default profile **start**. The administrator access is optional for all other routing workflows.



Every administrator access is protected from unauthorized access by an individual PIN. You can define this PIN in the general settings of the relevant Auto Attendant profile.

## 19.10 Configuring a Routing Workflow

This section describes the basic proceedings for configuring a new routing workflow for the OpenScape Auto Attendant.

The required steps are divided in the following sub-sections:

- 1) [Creating an Auto Attendant Profile](#)
- 2) [Defining general Profile Settings](#)
- 3) [Defining Error Handling Settings](#)
- 4) [Defining Operation Modes for the Routing Workflow](#)
- 5) [Configuring Access to the Routing Workflow](#)
- 6) [Configuring Access to the Administrator Access](#)
- 7) [Configuring a Routing Workflow for a Media Server Farm](#)

### 19.10.1 Creating an Auto Attendant Profile

---

**NOTICE:** You can use the already pre-set Auto Attendant profile **start** for configuring the first routing workflow for the OpenScape Auto Attendant. In this case you can skip the descriptions in this section and configure the Auto Attendant profile **start** in the ensuing sections.

---

You need to create a new Auto Attendant profile for configuring a new routing workflow for the OpenScape Auto Attendant.

#### Start the configuration

How to create a new Auto Attendant profile:

- 1) On the **Configuration** navigation tab of the Common Management Platform click on the **Unified Communications** navigation menu item.
- 2) In the navigation tree, click on **Configuration > Media Server**.

You see a list of all Media Servers available in the OpenScape system.

- 3) In the list select the OpenScape Media Server link that you want to configure.

The configuration dialog of the selected OpenScape Media Server opens.

- 4) In the configuration dialog switch to the **Applications** tab.

You see a list of all applications that are active in the selected OpenScape Media Server.

- 5) Select the **AutoAttendant** link in the list.

The configuration dialog of the OpenScape Auto Attendant plug-in opens. You see a list of all Auto Attendant profiles configured in the selected OpenScape Media Server.

- 6) Mark the radio button of the Auto Attendant profile **start** and select **Copy**.

The configuration dialog for a new Auto Attendant profile opens. The defaults for the new profile correspond to those of the Auto Attendant profile **start**.

- 7) Assign a name to the new Auto Attendant profile under **Profile name**.

*Example:* Sales\_Department

- 8) Select **Save**.

The configuration dialog for a new Auto Attendant profile closes and the list of all Auto Attendant profiles displays the new profile. This process may take some seconds.

## 19.10.2 Defining general Profile Settings

How to define the general settings for the routing workflow:

- 1) Mark the radio button of the created Auto Attendant profile and select **Edit**.

The configuration dialog for the selected Auto Attendant profile opens.

- 2) Verify that the **General** tab is displayed.
- 3) Select under **Default language** the language for playing greetings of the user and administrator access to callers.
- 4) Select the **Address translation context** to be used by the OpenScape Auto Attendant to normalize and localize phone numbers for the routing workflow.
- 5) If you wish to administer the workflow of the Auto Attendant profile restrictedly via an administrator access, execute the following steps:
  - a) Select the **Enable administrator mode** option.
  - b) Enter under **Administrator access PIN** a digit string that protects the administrator access from unauthorized access.

You have thus defined the general settings for the routing workflow.

## 19.10.3 Defining Error Handling Settings

Determine how the routing workflow is to react to incorrect caller entries by executing the following steps:

- 1) In the Auto Attendant profile configuration dialog switch to the **Error Handling** tab.
- 2) Specify under **Number of repetitions** how often a greeting can be consecutively played if a caller uses incorrect entries or does not react to input prompts at all.

When the specified number of repetitions is exceeded, the connection is closed or the caller is connected to an operator.

- 3) How to define the OpenScape Auto Attendant behavior for the event that the setting under **Number or repetitions** is exceeded:
  - For connecting the caller to the operator select the **Call operator in case of error** option.
  - For closing the connection to the caller leave the **Call operator in case of error** option unmarked.

You have thus defined how the routing workflow reacts to incorrect caller entries.

## 19.10.4 Defining Operation Modes for the Routing Workflow

The operation modes of a routing workflow determine how the routing workflow behaves against a caller. In this context, the OpenScape Auto Attendant offers a large number of operation modes and actions for adjusting the behavior of a routing workflow to individual requirements.

The example configuration of this section is restricted to the following selected operation modes.

- Within business hours
- Outside business hours
- On weekends

If you wish to configure additional operation modes, proceed basically as is described for the mentioned operation modes. Detailed information about all operation modes provides [Operation Mode Settings of Auto Attendant Profiles](#) on page 801.

### 19.10.4.1 Defining the Behavior for Business Hours

How to define the behavior of the routing workflow during business hours:

- 1) In the Auto Attendant profile configuration dialog switch to the **Operation Modes** tab.

You see a list of all operation modes configured for the Auto Attendant profile.

- 2) If the **Business hours** operation mode is not yet included in the list of configured operation modes, execute the following steps.

- a) Select **Add**.

The dialog for adding a new operation mode opens.

- b) Select under **Operation mode** the **Business hours** setting.

- c) Select **OK**.

The **Business hours** operation mode appears in the list of configured operation modes.

- 3) Mark the radio button of the **Business hours** operation mode and select **Edit**.

The configuration dialog of the selected operation mode opens.

- 4) Select the option **Business hours mode is active**.
- 5) Only leave working days checkmarked for which business hours exist.

---

**NOTICE:** If you wish to exclude time definitions from the **Business Hours** operation mode, you need to represent them by other operation modes – e.g. by the **Weekend** operation mode. If weekdays remain unconsidered during the configuration of an Auto Attendant profile, a note informs you accordingly when you save your settings. The OpenScape Auto Attendant uses the **Business Hours** operation mode for unconsidered days by default.

---

- 6) Set the respective business hours for each of the marked days under **Business Hours Start** and **Business Hours End**.

7) How to define the keypad layout for the specified business hours:

a) Select **Add**.

The dialog for adding a new key-action assignment opens.

b) Select under **Auto Attendant Action** the action to be offered to a caller during business hours.

Depending on the action you select, further settings may be displayed. In [Keypad Layout Settings of the Operation Modes](#) on page 808 you find information about these settings.

c) Select under **DTMF Key** the digit for a caller to reach the selected Auto Attendant action in the main menu of the user access.

d) Select **Save**.

The new key-action assignment is displayed in the keypad layout.

e) If required, create further key-action assignments for business hours in the same way.

8) Select **Save**.

You have thus defined the behavior of the routing workflow during business hours.

#### 19.10.4.2 Defining the Behavior outside Business Hours

How to define the behavior of the routing workflow outside business hours:

1) If the **Non-Business Hours** operation mode is not yet included in the list of configured operation modes, execute the following steps.

a) Select **Add**.

The dialog for adding a new operation mode opens.

b) Select under **Operation mode** the **Non-Business Hours** setting.

c) Select **OK**.

The **Non-Business Hours** operation mode appears in the list of configured operation modes.

2) Mark the radio button of the **Non-Business Hours** operation mode and select **Edit**.

The configuration dialog of the selected operation mode opens. You see the weekdays and times you have defined in the operation mode **Business hours**. All times that remained unconsidered for the listed weekdays apply for the operation mode **Non-Business Hours**.

3) Select the option **Non-business hours mode is active**.

- 4) If you wish to create a keypad layout for non-business hours, execute the following steps.

---

**NOTICE:** If you do not define a keypad layout, the caller hears a non-business-hours greeting during the relevant times and the connection is closed.

---

- a) Select the option **Keypad Layout Menu for the non-business hours**.
- b) Select **Add**.

The dialog for adding a new key-action assignment opens.

- c) Select under **Auto Attendant Action** the action to be offered to a caller outside business hours.

Depending on the action you select, further settings may be displayed. In [Keypad Layout Settings of the Operation Modes](#) on page 808 you find information about these settings.

- d) Select under **DTMF Key** the digit for a caller to reach the selected Auto Attendant action in the main menu of the user access.
- e) Select **Save**.

The new key-action assignment is displayed in the keypad layout.

- f) If required, create further key-action assignments for non-business hours in the same way.

- 5) Select **Save**.

#### 19.10.4.3 Defining the Behavior for Weekends

How to define the behavior of the routing workflow on weekends:

- 1) If the **Weekend** operation mode is not yet included in the list of configured operation modes, execute the following steps.

- a) Select **Add**.

The dialog for adding a new operation mode opens.

- b) Select under **Operation mode** the **Weekend** setting.
- c) Select **OK**.

The **Weekend** operation mode appears in the list of configured operation modes.

- 2) Mark the radio button of the **Weekend** operation mode and select **Edit**.

The configuration dialog of the selected operation mode opens. All weekdays you have not defined in the operation mode **Business hours** are offered for selection.

- 3) Tick the checkboxes of all offered weekdays.

---

**NOTICE:** If weekdays remain unconsidered during the configuration of an Auto Attendant profile, a note informs you accordingly when you save your settings. The OpenScape Auto Attendant uses the **Business Hours** operation mode for unconsidered days by default.

---

- 4) If you wish to create a keypad layout for weekends, execute the following steps.

---

**NOTICE:** If you do not define a keypad layout, the caller hears a weekend greeting during the relevant times and the connection is closed.

---

- a) Select the option **Keypad Layout Menu for the weekend**.
- b) Select **Add**.

The dialog for adding a new key-action assignment opens.

- c) Select under **Auto Attendant Action** the action to be offered to a caller during a weekend.

Depending on the action you select, further settings may be displayed. In [Keypad Layout Settings of the Operation Modes](#) on page 808 you find information about these settings.

- d) Select under **DTMF Key** the digit for a caller to reach the selected Auto Attendant action in the main menu of the user access.
- e) Select **Save**.

The new key-action assignment is displayed in the keypad layout.

- f) If required, create further key-action assignments for weekends in the same way.
- 5) Click on **Save** to save the modifications for the operation mode.
- 6) Click on **Save** to save the modifications for the Auto Attendant profile.

---

**NOTICE:** If weekdays remain unconsidered during the configuration of an Auto Attendant profile, a note informs you accordingly when you save your settings. The OpenScape Auto Attendant uses the **Business Hours** operation mode for unconsidered days by default.

---

You have thus defined the behavior of the routing workflow.

### 19.10.5 Configuring Access to the Routing Workflow

You need to create a new Media Server terminal to enable callers reaching the new routing workflow. You need to assign the routing workflow to this terminal and the phone number, under which the routing workflow shall be available.

#### Start the configuration

How to create a new terminal:

- 1) In the configuration dialog of the selected OpenScape Media Server switch to the **Terminals** tab.

You see a list of all terminals that are active in the selected OpenScape Media Server.

- 2) Select **Add**.

The configuration dialog for the terminal opens.

- 3) Specify a unique identifier for the terminal under **Terminal ID**. Under this identifier the terminal is administered in the Common Management Platform.

- 4) Select the following application under **Application**:

**AutoAttendant#<profile name >**

- 5) Select **SIP**.

The configuration dialog for the SIP settings opens.

- 6) Select an SIP server line under **Outbound line**.

This SIP server line is used for signaling outbound communication connections for the selected application.

- 7) Select **Save** to save the settings and to close the dialog.
- 8) Execute the following steps to bind at least one phone number to the terminal:

---

**NOTICE:** If you wish to define several phone numbers that cannot be specified in the form of a single phone number expression, you need to bind at least one more address to the terminal.

---

- a) Click on **Add** in the **Addresses** section.

The configuration dialog for an address opens.

- b) Specify under **Address-expression** the desired phone number expression.

This expression defines the phone numbers under which the selected terminal is to be available in the OpenScape Media Server.

---

**NOTICE:** Always specify the phone number in normalized phone number format – e. g. +492404901100.

---



---

**NOTICE:** You need to ensure that the phone numbers configured here are routed in the communications system to the SIP trunk that leads to the OpenScape Media Server.

---

- c) Determine under **Type** in which format the specified phone number expression is to be interpreted by the OpenScape Media Server.
  - d) Click on **OK** to copy the address settings.
  - e) If required, bind further addresses to the terminal in the described manner.
- 9) Click on **Save** to copy the settings for the terminal.

Callers can thus reach the new routing workflow in the selected OpenScape Media Server under the specified phone number.

Further details about the settings of a terminal provides the manual *OpenScape Media Server, Administrator Documentation*.

## 19.10.6 Configuring Access to the Administrator Access

If you have activated the administrator mode in the general settings of the Auto Attendant profile, you need to make this administrator mode available. You need to create a new Media Server terminal for this purpose. Then, you need to

assign the relevant administrator access to this terminal and the phone number, under which the administrator access shall be available.

Proceed basically in the same way as is described in [Configuring Access to the Routing Workflow](#) on page 818. Use AutoAttendant#<profile name>Admin instead of the application AutoAttendant#<profile name>.

### 19.10.7 Configuring a Routing Workflow for a Media Server Farm

Large Deployment uses several OpenScape Media Servers in a Media Server farm. Such a Media Server farm can comprise up to four OpenScape Media Servers.

If you wish to configure the routing workflow to be present of every Media Server of a Media Server farm, you need to execute the steps of the following guide:

- 1) You need to configure the new Auto Attendant profile for all OpenScape Media Servers of the Media Server farm.
- 2) You need to configure all Media Servers of the Media Server farm and the communications system as you need to for the voice portal. You find details about this configuration in [Configuring the Voice Portal for Media Server Farm](#) on page 189.



## 20 Displaying Directory Numbers in the UC Application Clients

The client used determines how a directory number is displayed to a user for example in the call journal of his/her UC Application client. For the time being, there are two basic types of displaying directory numbers:

- Displaying a transferred directory number In this case the UC Application client displays directory numbers exactly as the OpenScape Voice or OpenScape 4000 communications system transfers them as display information to OpenScape UC Application. Displaying a prepared directory number In this case a directory number is displayed as follows:
  - If the directory number can be resolved into a contact, it is displayed in the form of the associated contact name. The only exception from this rule are directory numbers of subscribers who are assigned to a multi-line hunt group (MLHG) of OpenScape Voice.
  - If the directory number cannot be resolved into a contact, it is displayed in the form of a normal directory number. The only exception from this rule are directory numbers of subscribers who are assigned to a multi-line hunt group (MLHG) of OpenScape Voice.
  - If the directory number is assigned to a multi-line hunt group (MLHG) of OpenScape Voice, it is displayed as normalized pilot directory number of the relevant multi-line hunt group (MLHG).

The UC Application client used determines which of these directory number displays are deployed.

The following clients display transferred directory numbers:

- OpenScape Fusion clients
- OpenScape Mobile Client

The following clients display prepared directory numbers:

- OpenScape Web Client
- OpenScape Desktop Client in the display mode of OpenScape Web Client
- OpenScape Desktop Integration, if downloaded via OpenScape Web Client

## 21 Call Journal / Call History Model of OpenScape Web Client

### 21.1 Call History Model for OpenScape Web Client

The information displayed in the OpenScape Web Client Call History follows these principles:

- Each call from the user's perspective creates exactly one call history entry.
- In case a call is forwarded or transferred several times the system stores only the first and last connection.
- The status of a call history entry always results from the status of the last connection.
- All answered calls have a duration greater than 0 seconds.
- In case a call is transferred, the calculation of its duration starts when any party answers the call. The transfer of an answered call doesn't reset the duration.
- Since V9, sequential calls from the same person (as long as there is no call from another person in between) are grouped into one entry with the number of calls in paranthesis.

OpenScape Web Client users need to click into the grouped entry in order to see the details of each single call entry.

### 21.2 Descriptions in journal / call history entries

The following descriptions are used in call journal entries of OpenScape Web Client:

**Table 18: Descriptions in call journal / call history entries**

| Description                     | Meaning                                                                        | Call Scenarios                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Picked up from:<br><subscriber> | A call coming in for the user was accepted by another subscriber.              | <ul style="list-style-type: none"><li>• Pickup (not in the Team function scope)</li></ul>                                                                                                   |
| Accepted from:<br><subscriber>  | A call made by the user was forwarded to and accepted from another subscriber. | <ul style="list-style-type: none"><li>• Forward</li><li>• Deflect</li><li>• Single Step Transfer</li><li>• Consult and Transfer</li><li>• Multi Line Hunt Group of OpenScape 4000</li></ul> |

| Description                    | Meaning                                                                            | Call Scenarios                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accepted for:<br><subscriber>  | Incoming call forwarded to the user by another subscriber and accepted.            | <ul style="list-style-type: none"> <li>• Forward</li> <li>• Deflect</li> <li>• Single Step Transfer</li> <li>• Consult and Transfer</li> <li>• Multi Line Hunt Group of OpenScape 4000</li> </ul> |
| Redirected to:<br><subscriber> | A call made by the user was forwarded to and not accepted from another subscriber. | <ul style="list-style-type: none"> <li>• Forward</li> <li>• Deflect</li> <li>• Single Step Transfer</li> <li>• Consult and Transfer</li> <li>• Multi Line Hunt Group of OpenScape 4000</li> </ul> |
| Forwarded to:<br><subscriber>  | Incoming call forwarded to another subscriber by the user.                         | <ul style="list-style-type: none"> <li>• Forward</li> <li>• Deflect</li> <li>• Single Step Transfer</li> <li>• Consult and Transfer</li> <li>• Multi Line Hunt Group</li> </ul>                   |
| Forwarded:<br><subscriber>     | Incoming call forwarded to the user by another subscriber and not accepted.        | <ul style="list-style-type: none"> <li>• Forward</li> <li>• Deflect</li> <li>• Single Step Transfer</li> <li>• Consult and Transfer</li> <li>• Multi Line Hunt Group</li> </ul>                   |

## 22 Provisioning via LDAP Directories

By means of the SPML interface of OpenScape UC Application you can import data to the UC Application system.

A detailed description of the SPML interface and how you can use it to import data to the UC Application system is available in the manual *OpenScape UC Application SPML SDK, Programming Guide* in chapter 3 *Provisioning LDAP Directories*.

## 23 Adding an External Language in Integrated Simplex

The following languages are available for a number of packages in an Integrated Simplex deployment in UC V11:

**Table 19: Overview Packages and Languages for Integrated Simplex**

| Available Package                          | Language   | Code  |
|--------------------------------------------|------------|-------|
| mediaserver announcements                  | German     | de_de |
| mediaserver_voiceportal_languagepack       | Finish     | fi_fi |
| mediaserver_autoattendant_languagepack     | French     | fr_fr |
| mediaserver_voiceportalspeech_languagepack | Italian    | it_it |
| scs_conferencing_languagepack              | Japanese   | ja_jp |
| uc-tts                                     | Flemish    | nl_be |
| uc-asr                                     | Polish     | pl_pl |
|                                            | Brazilian  | pt_br |
|                                            | Portuguese | pt_pt |
|                                            | Russian    | ru_ru |
|                                            | Chinese    | zh_cn |

You can add an external language as follows:

- 1) "Load" the additional languages. Create a combined repository by issuing the command:

```
osc-setup cr -b /nfsmount/CI-IS0s/
V9R1.0.0-030000/OpenScapeUcSuiteApps-BasePackage-
V9R1.0.0-030000.iso /nfsmount/CI-IS0s/V9R1.0.2-030002/
OpenScapeUcSuiteApps_PATCH-V9R1.0.2-030002.iso -l /tmp/
repo
```

- 2) Add the language for the package you want, by issuing the following commands:

```
cd /tmp/repo ./support/installIntegratedSimplex.sh addLang <package>
<code>
```

For example, should you want to load the German language (code = de\_de) for the package uc - tts, execute type:

```
./support/installIntegratedSimplex.sh addLang uc-tts de_de
```

## 24 HAProxy Manager Tool

The HAProxy Manager Tool is used to configure the parameters and settings of HAProxy. HAProxy configuration is stored in the haproxy.cfg file, which is located at: /usr/share/haproxy

---

**IMPORTANT:** It is not recommended to manually edit haproxy.cfg file. Use the HAProxy Manager Tool instead.

---

---

**NOTICE:** 150000 maximal connections per Listener are used. This is configured in the tool, you cannot change it.

---

### 24.1 Basic Options

Before you can use the HAProxy Manager Tool, you need to verify that HAProxy is installed. Therefore, type the following command as root user:

```
rpm -qa | grep -i haproxy
```

You should see something like: haproxy-1.2.3-1 (the numbers can be different, depending on the version installed).

In order to run HAProxy Manager Tool, type the following command as root user:

```
haproxymanager
```

HAProxy Manager Tool starts and a welcome screen opens. Hereby you see instructions on how to choose an option among the available list offered by the tool. The instructions are:

Use:

- CURSOR to go UP, DOWN,
- LEFT and RIGHT to navigate,
- SPACE to select, and
- RETURN to confirm

---

**NOTICE:** In some cases, a mouse works as well.

---

When there is no configuration, the Discard & configure HAProxy option is automatically selected for you, so that you provide a configuration for the Reverse Proxy (HAProxy). You are asked several questions to appropriately configure the Reverse Proxy (HAProxy) (see [Discard and configure HAProxy](#) on page 827).

In any other case, you get into the main menu. The menu has the following options:

- 1) Discard & configure HAProxy
- 2) Discard Facade/Web Client configuration
- 3) Configure Web Collaboration
- 4) Discard existing Web Collaboration configuration
- 5) Show current configuration

- 6) Restart HAProxy
- 7) About HAProxy
- 8) Exit

When you get to the main menu, and before you make any change, it is highly recommended to choose the option 5) [Show current configuration](#).

When you have the system configured (Reverse Proxy/HAProxy, Facade/Web Client, Web Collaboration connectors), then you should restart the Reverse Proxy (HAProxy) (choose the option 6).

---

#### IMPORTANT:

When you have upgraded from an older version (e.g. V7R3) and you face problems (a possible reason could be that you have changed deployment) then you may need to reconfigure from scratch.

Before you drop the connectors, make a copy / backup of the file `/usr/share/haproxy/haproxy.cfg`.

Select Discard existing Web Collaboration Configuration (4) and then Discard Facade / Web Client Configuration (2). Then continue with Discard & configure HAProxy. Finally you need to restart the HAProxy (8).

---

### 24.1.1 Discard and configure HAProxy

Choose this option to create a configuration for the Reverse Proxy (HAProxy). For this, you are asked several questions and depending on the answers you provide, the configuration file is generated/updated.

---

**NOTICE:** Existing Web Collaboration Connectors are not removed..

---

For answering the questions, you need to provide previously-known:

- Standalone Server or Facade Server

---

**NOTICE:** A Facade Server is only needed when at least one mobile user (OSMO) is used. In case that there is no mobile user, select the Standalone. Standalone serves Web Collaboration and Internet Access for Web Client and Fusion for Office.

---

- WebClient Address

In case you create a Listener (recommended) you need, also, to provide previously-known:

- Listener IP Address (HAProxy IP Address)
- Listener Port (HAProxy port)
- Web Collaboration IP Address (where requests will be sent)
- Web Collaboration Port

- a certificate (pem-file) in case you have secure connection and you do not want to use self-signed certificate.

Finally, you specify a name for the listener.

---

**NOTICE:** The name for the Web Collaboration Connector must be unique.

---

## 24.1.2 Discard Facade / Web Client configuration

Choose this option to remove the Facade / Web Client configuration.

---

**IMPORTANT:** When you discard the Facade Web Client configuration, this operation cannot be undone. If you want to recreate the Facade Web Client configuration, you need to do this from scratch via the [Discard and configure HAProxy](#) option.

---

## 24.1.3 Show current configuration

Choose this option to view information about the current Facade configuration and Web Collaboration.

## 24.1.4 Restart HAProxy

Choose this option to restart HAProxy. You are informed about the status.

## 24.1.5 About HAProxy

Choose this option to view a general description of HAProxy. Information about the current version of HAProxy is also displayed.

## 24.2 Creating certificates without password protection for HAProxy unattended startup

HAProxy does not support automated startup with password protected certificates. In cases where password protected certificates are used, users are prompted to enter the password during the start up of the process. To allow for an unattended automatic startup of HAProxy e.g. after a system reboot, a certificate without password needs to be used and stored in a secure location.

A password-less certificate for HAProxy can be generated from the customer's PKCS12 keystore already used in the Facade server.

Transfer the p12 file under a temporary working directory and execute the following:

- 1) Backup the keystore file:

```
cp keystore-file.p12 keystore-file.p12.orig
```



## 2) Extract the server certificate:

```
openssl pkcs12 -clcerts -nokeys -in "YourPKCSFile" -out certificate.crt -
password pass:PASSWORD -passin pass:PASSWORD
```

## 3) Extract the CA (Root, Intermediate) certificates:

```
openssl pkcs12 -cacerts -nokeys -in "YourPKCSFile" -out ca-cert.ca -
password pass:PASSWORD -passin pass:PASSWORD
```

---

**NOTICE:** Check if the exported file (ca-cert.ca) contains the CA certificates (Root, Intermediate) and is not 0 bytes. This needs to be done because some times .pfx and .p12 files are received with just a server certificate and the CA certificates should be added additionally.

---

## 4) Extract the private key (use a temporary password):

```
openssl pkcs12 -nocerts -in "YourPKCSFile" -out private.key -
password pass:PASSWORD -passin pass:PASSWORD -passout
pass:TemporaryPassword
```

## 5) Remove the passphrase:

```
openssl rsa -in private.key -out "NewKeyFile.key" -passin
pass:TemporaryPassword
```

## 6) Cat the files in the following order to create the new password-less certificate. This is the new certificate that you want to use with HAProxy.

- Private key without Passphrase
- Server-Certificate
- Intermediate-CA certificate
- Root-CA certificate

For example:

```
cat "NewKeyFile.key" > HAProxy_nopass_cert.pem
```

```
cat "certificate.crt" >> HAProxy_nopass_cert.pem
```

```
cat "ca-cert.ca" >> HAProxy_nopass_cert.pem
```

At this point the password-less certificate HAProxy\_nopass\_cert.pem generation is completed and it can be defined during the set-up wizard when executing the haproxymanager.

Optional step:

## 7) You can now also create a new password-less PKCS12 file:

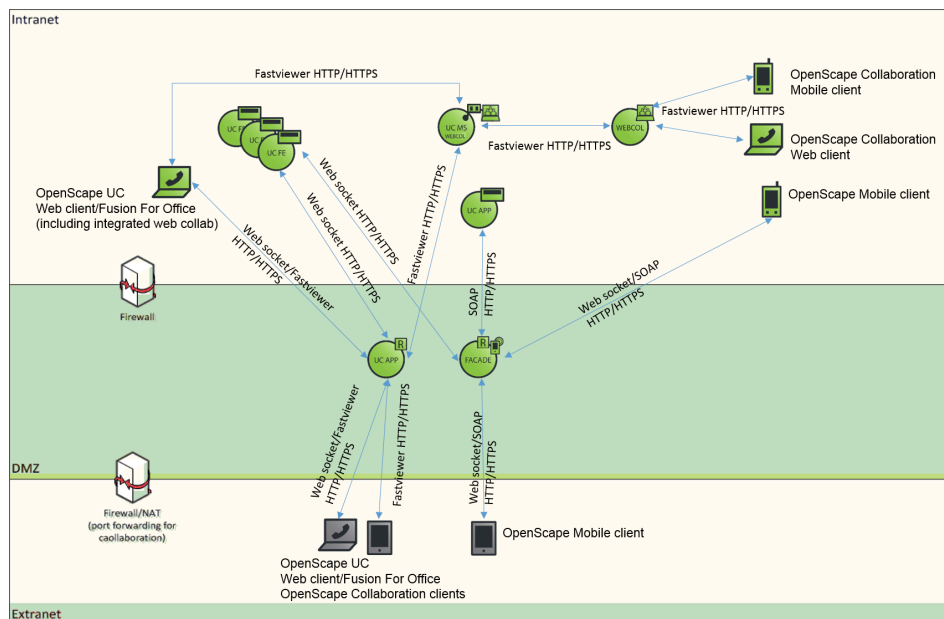
```
openssl pkcs12 -export -nodes -CAfile ca-cert.ca -in
HAProxy_nopass_cert.pem -out "NewPKCSWithoutPassphraseFile"
```

---

**IMPORTANT:** The newly created certificate without password protection needs to be stored in a secure location on the system that hosts the HAProxy i.e. a root access only directory. The proposed directory is /root. This way the certificate will be secure as only root user can access this directory. This certificate should NOT be stored under the default HAProxy path /usr/share/haproxy. After creating the password-less certificate and transferring it to the secure location, please remove completely the previously used temporary working directory and all of its contents.

---

## 25 Configuring Internet Access of OpenScape UC clients



This feature is only released for OpenScape UC Fusion for Office V1.1 and Web Client.

This feature offers UC clients (here Fusion for Office and Web Client) to use internet access without a VPN connection (similar to Outlook).

When there are no mobile users, the Standalone server is used (UC App). The facade server is only necessary when mobile devices need to be used (should not be the case here).

The Reverse proxy is either on the Facade server or on the UC-App server.

**NOTICE:** The SIP softphone part of Fusion for Office client needs to connect through the SBC.

## 26 Reverse Proxy deployment information

- Reverse Proxy on Facade serves mobile traffic for all deployments. If there are more than one Facade servers each of them will have a Reverse proxy which will handle the OSMO Call control events for this node.
- In case OpenScape Mobile Pro (OSMO Pro) is used, then a Reverse Proxy is mandatory and it must be configured accordingly.
- Web Collaboration and Internet Access can be served by a Standalone node for integrated/small/large/very large deployments.
- In case of small or integrated deployment the Facade server may also handle the Web Collaboration and Internet Access to UC Clients. (There is no need for a separate Standalone server)

## IPv6 Support

Prerequisites for installing UC on a IPv6 or IPv4 with IPv6 mixed system

# 27 IPV6 Support

With V11, IPv6 is supported.

## 27.1 Prerequisites for installing UC on a IPv6 or IPv4 with IPv6 mixed system

The IP Configuration should look like below (IPv6 only system):

```
uctest4:~ # ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:56:90:68:76
 inet6 addr: fd00:10:11:246:e81d:ed37:785d:9032/64 Scope:Global
 inet6 addr: fd00:10:11:246:4c12:1c91:8c3b:849f/64 Scope:Global
 inet6 addr: fd00:10:11:246:d9ad:508f:e1f8:410d/64 Scope:Global
 inet6 addr: fd00:10:11:246:995f:e5a:dc26:d24b/64 Scope:Global
 inet6 addr: fd00:10:11:246:250:56ff:fe90:6b76/64 Scope:Global
 inet6 addr: fd00:10:11:246:5d33:7ecb:a767:d2fb/64 Scope:Global
 inet6 addr: fe80::250:56ff:fe90:6b76/64 Scope:Link
 inet6 addr: fd00:10:11:246:1e6:8482:dd51:4642/64 Scope:Global
 inet6 addr: fe80::a0b:f62d/24 Scope:Link
 inet6 addr: fd00:10:11:246:648d:a2c7:6852:9c5a/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:1796306 errors:0 dropped:2064 overruns:0 frame:0
 TX packets:4373 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:159141568 (151.7 Mb) TX bytes:357582 (349.2 Kb)
```

The IPv6 scope should be **global**

```
eth1 Link encap:Ethernet HWaddr 00:50:56:90:22:D8
 inet addr:10.11.246.46 Bcast:10.11.246.255 Mask:255.255.255.0
 inet6 addr: fd00:10:11:246:29b5:afbe:6aef:757f/64 Scope:Global
 inet6 addr: fd00:10:11:246:5cb0:81f7:948d:9b4c/64 Scope:Global
 inet6 addr: fe80::250:56ff:fe90:22d8/64 Scope:Link
 inet6 addr: fd00:10:11:246:1d75:1696:d31c:7638/64 Scope:Global
 inet6 addr: fd00:10:11:246:648b:17a3:5912:184d/64 Scope:Global
 inet6 addr: fd00:10:11:246:5894:6168:acac:164b/64 Scope:Global
 inet6 addr: fd00:10:11:246:4c63:4bd4:edee:16c7/64 Scope:Global
 inet6 addr: fd00:10:11:246:5409:f28:850f:13b6/64 Scope:Global
 inet6 addr: fd00:10:11:246:250:56ff:fe90:22d8/64 Scope:Global
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:17590618 errors:0 dropped:2060 overruns:0 frame:0
 TX packets:2165874 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:2000097323 (1907.4 Mb) TX bytes:194666075 (185.6 Mb)
```

The system will be still accessible via IPv4

## 27.2 Activating IPv6 on a SLES system via yast:

---

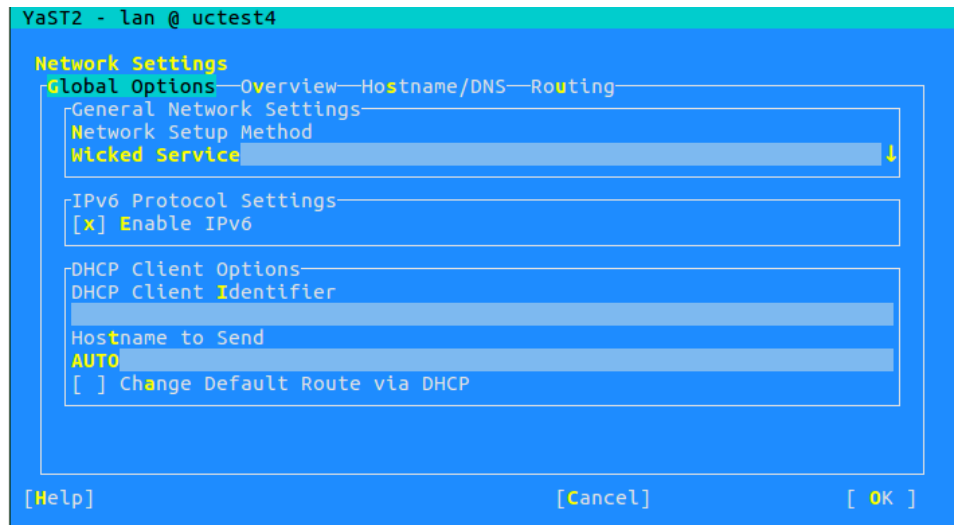
### NOTICE:

Depending on your OpenScape UC version, your operating system must be:

- SLES 12 SP5, for UC V11R5
  - SLES 15 SP5, for UC V11R6
- 

- 1) Navigate to: **Network Devices -> Network Settings -> Global Options -> Enable IPv6**
- 2) Check if **Enable IPv6** is marked.

- 3) Click **OK**.
- 4) Reboot your system.



## 27.3 Configuring knut.response.file

In opposite to IPv4 configuration the IPv6 address should be embraced with brackets.

```
Administrator logon password
please respect the password policy rules (...)
SI_SYMPHONIA_ADMIN_PASSWORD=Asd123!

Unique Identifier of the system
charset [A-Za-z0-9_], the '_' not at the front or the end
SI_COMMUNITY_NAME=uctest4com

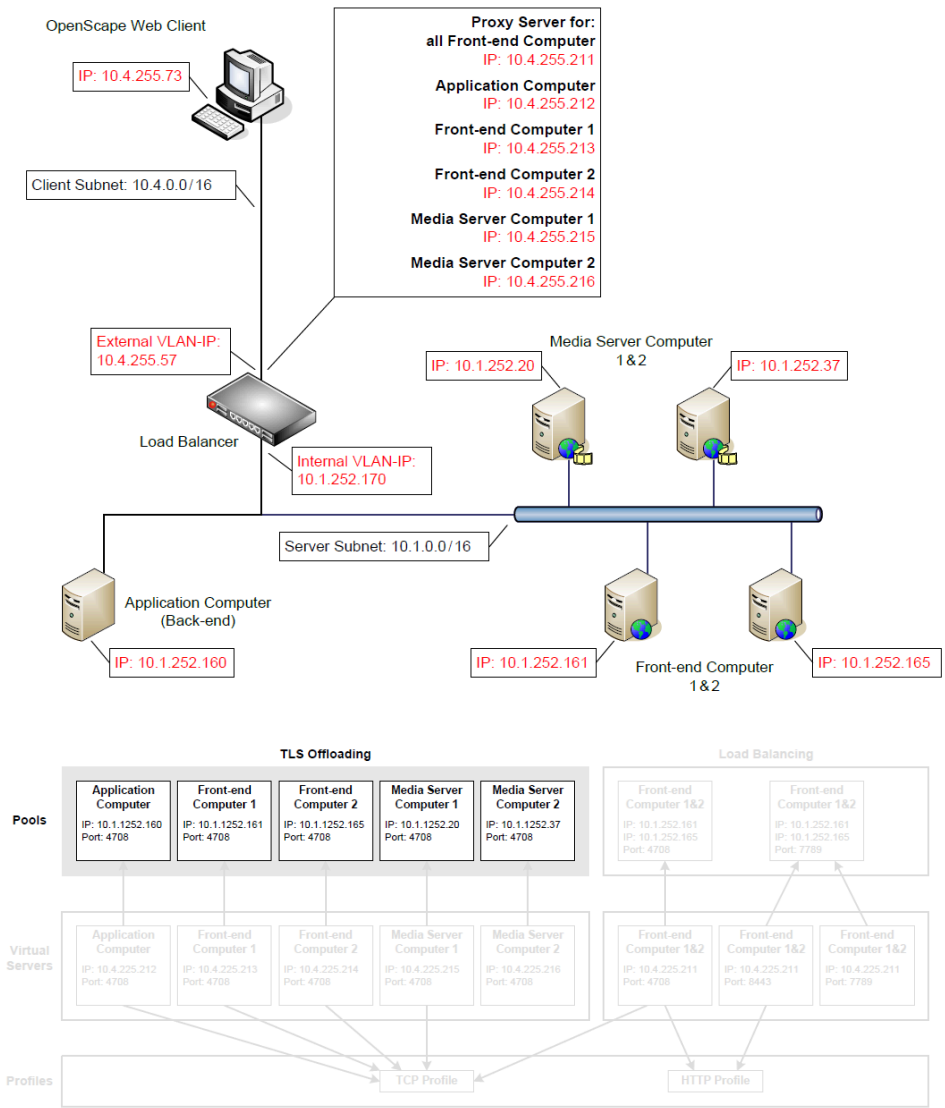
The hostname or ip address of the primary node
charset [a-z0-9-](hostname) (or for ip [0-9.])
SI_PRIMARY_NODE_HOST=[fd00:10:11:246:250:56ff:fe90:627e]

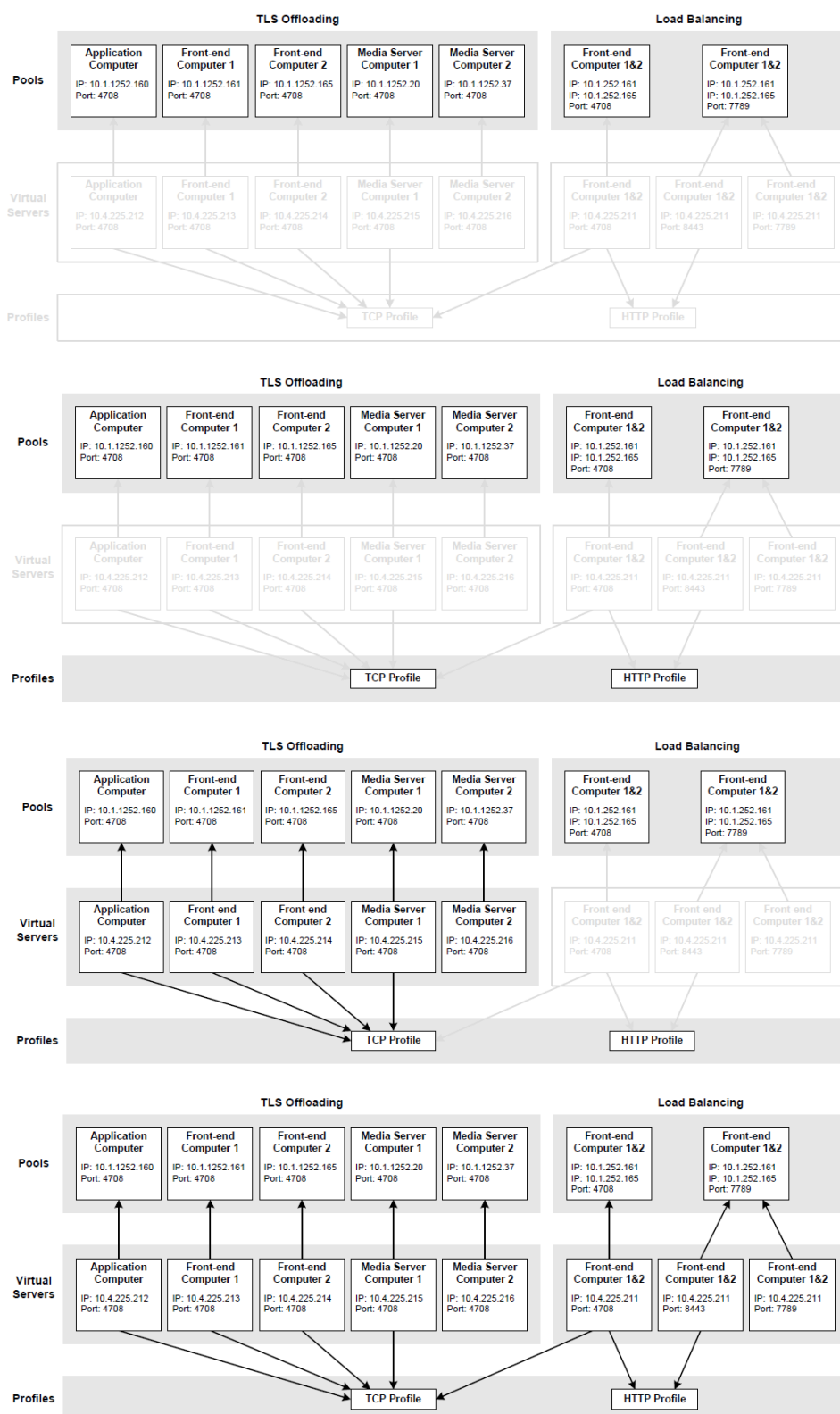
The hostname or ip address of the local node
charset [a-z0-9-](hostname) (or for ip [0-9.])
SI_LOCAL_HOST=[fd00:10:11:246:250:56ff:fe90:627e]
```

28 Appendix

This section contains additional reference information.

28.1 Overview of the UC Application components that concern the load balancer





# Index

## A

Application computer  
    activating Framework port 4708 [588](#)  
AutoAttendant  
    CMP settings [796](#)  
AutoAttendant plug-in [796](#)

## B

Backing up [448](#)  
Backup [448](#)  
Busy signaling  
    activating [559](#)  
    concept [559](#)  
Busy-on-Busy  
    activating [559](#)  
    concept [559](#)

## C

changeSFWip.sh [582](#)  
Changing music-on-hold for conference portal [470](#)  
Changing the deployment scenario  
    Integrated Simplex to Standard Duplex (small) [94](#)  
    Standard Duplex (small) to (large) [94](#)  
    within Standard Duplex (large) [95](#)  
CMP  
    backing up [448](#)  
    backup [448](#)  
    groupware service management [425](#)  
    managing instant messaging connections [445](#)  
    restore [448](#)  
    restoring [448](#)  
collect.sh [615](#)  
Coman [775](#)  
conference management tool Coman [775](#)  
Conference portal [31](#)  
    calloutGracePeriod [766](#)  
    changing music-on-hold [470](#)  
    CMP settings [737](#)  
    Coman tool [775](#)  
    configuring participant signaling [475](#)  
    configuring video layouts [476](#)  
    dtmfConfig [766](#)  
    dtmfKeyDelay [766](#)  
    fastTransfer [767](#)  
    fastWelcome [767](#)  
    forceVideoConferences [598](#)  
    language [767](#)  
    managing [467](#)  
    max. number of participants [472](#)  
    maximalParticipants [768](#)  
    neutralWelcome [768](#)

    rejoinGracePeriod [768](#)  
    security settings outgoing connections [468](#)  
    statistics data [631](#)  
    systemwide video conference [598](#)  
    video layout management [769](#)  
conference portal plug-in [737](#)  
Configuring default language for voice portal [465](#)  
Configuring HTTPS port for CMP [587](#)  
Configuring IPv6 support [587](#)  
configuring participant signaling [475](#)  
Configuring security settings for conference portal [468](#)  
Configuring video layouts [476](#)  
Connection  
    Exchange (2003) [32](#)  
    Exchange (2007) [32](#)  
    instant messaging [35](#)  
    LDAP [35](#)  
    Openfire [35](#)

## D

Dashboard [340](#)  
Data structure of the domain management [714](#)  
Deployment scenario  
    changing [94](#)  
    system relation [25](#)  
Domain management data [714](#)  
    access [714](#)  
    data structure [718](#)  
    editing a CSV file [715](#)

## E

ENG  
    Accepted for [823](#)  
    Accepted from [822](#)  
    Forwarded [823](#)  
    Forwarded to [823](#)  
    Picked up from [822](#)  
    Redirected to [823](#)  
    Set as default context [142](#)  
    Use Domain to Business Group Mapping [122](#)  
Exchange 2013 [425](#)  
Exchange 2016 [425](#)  
Exchange connection (2003) [32](#)  
Exchange connection (2007) [32](#)  
Exchange connection (2010) [32](#)  
Exchange provider (SMTP)  
    displaying [433](#)  
    editing [433](#)



## F

Facade server  
    configuring SSL [505](#)  
    parameter  
        https [502](#)

## G

GAL [426](#)  
Global address list [426](#)  
Groupware service  
    configuring encrypted transmission [435](#)  
    logging [618](#)  
    managing [425](#)

## H

Handling Groupware Exchange Contact Pictures [444](#)  
https [502](#)

## I

Instant messaging  
    managing [445](#)  
Instant-messaging connection [35](#)  
IPsec Configuration [691](#)

## L

LDAP connection [35](#)  
Limiting the number of conference participants [472](#)  
Logging  
    desktop integration tool [627](#)  
    groupware service [618](#)  
    Nuance Vocalizer (TTS) [630](#)  
    OpenScape 4000 [618](#)  
    OpenScape UC Application [608](#)  
    OpenScape Voice [617](#)  
    web server [622](#)  
    WebClient [622](#)  
Logging OpenScape 4000 [618](#)  
Logging OpenScape Voice [617](#)  
Logging the desktop integration tool [627](#)  
Logging TTS system [630](#)  
Logging web server [622](#)  
Logging WebClient [622](#)  
Lotus Domino [425](#), [425](#)

## N

NAT [592](#)  
NAT mapping tables [592](#)  
Notification  
    configuring for conferences [761](#)

## O

one-number service [30](#)  
One-number service (ONS) [30](#)  
ONS [30](#)  
Openfire connection [35](#)  
OpenScape Desktop Integration [483](#), [483](#)  
OpenScape Media Server  
    managing [479](#)  
OpenScape UC Application  
    logging [608](#)  
OpenScape Web Client  
    managing [479](#)

## P

Password policies  
    parameter  
        LockoutTime [575](#)  
        MaximumAge [573](#)  
        MaximumFailedAttempts [574](#)  
        MaximumLength [574](#)  
        MaximumRepeatedCharacters [574](#)  
        MinimumAge [573](#)  
        MinimumDigits [574](#)  
        MinimumLength [574](#)  
        MinimumSpecialCharacters [574](#)  
        MinimumUpperCaseCharacters [574](#)  
        PasswordHistoryDepth [574](#)

PIN [149](#)

PIN policies  
    parameter  
        LockoutTime [579](#)  
        MaximumAge [578](#)  
        MaximumFailedAttempts [579](#)  
        MaximumLength [578](#)  
        MaximumRepeatedCharacters [578](#)  
        MinimumAge [578](#)  
        MinimumDigits [578](#)  
        MinimumLength [578](#)  
        MinimumSpecialCharacters [578](#)  
        MinimumUpperCaseCharacters [578](#)  
        PasswordHistoryDepth [579](#)

## R

Restore [448](#)  
    OpenScape Voice (Standard Duplex) [460](#)  
Restoring [448](#)

## S

Save security certificate for CMP [569](#)  
Securing the groupware connection [435](#)  
Statistics data  
    conference portal [631](#)  
    OpenScape Media Server [644](#)  
Synchronize license assignments [580](#)

## T

Translating network addresses [592](#)

## U

UC-Application-Knoten [340](#)

Using Windows login data  
concept [547](#)

## V

Video layout management [769](#)

Voice portal

    CMP settings [728](#)

    configuring the default language [465](#)

    managing [462](#)

Voice portal plug-in [728](#)

## W

WebServer components

    managing [479](#)

